Security Metrics for a Business Information System

T.Chandrakumar
Thiagarajar College of Engineering, Madurai.

S. Parthasarathy, Ph.D
Thiagarajar College of Engineering, Madurai.

R Maragathameena
Thiagarajar College of Engineering, Madurai.

S Arun Raj Pandian
Thiagarajar College of Engineering, Madurai.

ABSTRACT

The notion of security metrics is a very significant aspect for Enterprise information System (BIS). Information Security metrics are often underused and in some cases unseen, anyway could be a profitable instrument in assembling better enterprise security. This information aides measure the day by day impact and quality of current defends and shows the quality of these functions through all business methodologies. This paper discusses a ASPIRE methodical approach to identify the right metrics to measure security preparedness and move toward a strong justification for information security investment and better enterprise outcomes.

Keywords

Information Security, Security metrics, Business Information Systems (BIS)

1. INTRODUCTION

Enterprises are facing an unprecedented threat environment. Cyber attacks are progressively complicated and change on an almost every day cornerstone. Yet, qualified information security is frequently underestimated furthermore, accordingly, frequently fails to offer the plan and assets to truly battle potential dangers. According to the National Institute of Standards and Technology (NIST), "Metrics are tools designed to facilitate decision-making and improve performance and accountability through collection, analysis, and reporting of relevant performance-related data [4]. The security metrics can be used to achieve the following goals: To evaluate presentation and to optimize protection level, to set up a reference grade about monitoring and enhancement of the organizational security level, to justify the budgets related to the information Security, Etc. Information security is an organizational operation where victories proceed unnoticed, but failures are embarrassingly public. To the untrained eye, security people, technologies, and method cost a lot of money, but produce little substantial yield on a daily basis, other than a vaguely satisfied feeling that "nothing awful happened" today. Information security metrics can assist in prioritizing

using choices dependent upon business risks and can additionally help champion and legitimize choices to the business. Effective information security metrics can clearly show the business impact of security, thus making the case for integrating the security function as feature of all business processes. This methodology can make organizations address related threats in a way that is both progressive and economical. Metrics can offer assistance answer the truly hard inquiries being asked today to justify any new security investment:

• Does it make us more secure today than we were before?

• How would we measure up to others in this industry?

• Are we suitably equalizing expense, hazard, furthermore convenience?

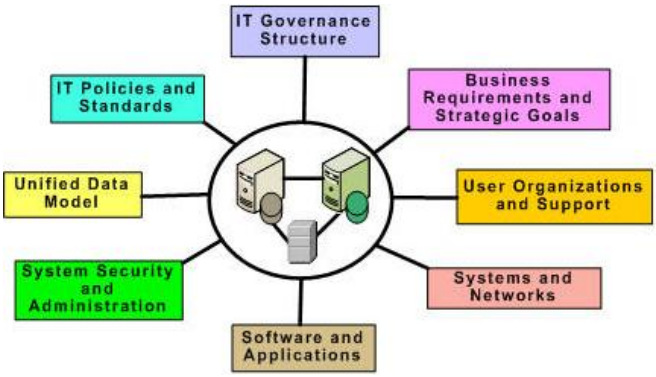

Figure 1. Enterprise Information System and its Elements

Enterprise information system architecture is a unified framework for managing and operating information systems and resources in an organization-wide setting. Enterprise information system architectures are designed and built based on the following major principles:

• Focus on organization-wide business needs and long-term strategic goals
• Data and infrastructure as an investment with long-term value and benefits
• System integration through sound design and use of applicable IT standards
• Coordination, collaboration, and shared resources (data, systems, applications, support)

2. LITERATURE REVIEW

The aim of information security is to ensure business continuity and minimize business damage by preventing and minimizing the impact of security incidents [1]. Information is an important business asset in today's enterprises. Hence enterprise information security is an important system quality that must be carefully managed [2].Managing something that is not measured is difficult to near impossible and Information Security is not an exception [3]. The evaluation of information systems security is a process in which the evidence for assurance is identified, gathered, and analyzed against criteria for security functionality and assurance level [4]. Security metrics are important indicators of how well security services are present in the information system and can be used to measure organization's security maturity level. Security metrics is tool that facilitates improved understanding, performance, Coverage, and decision making of various security processes, mechanisms and procedures [5].Metrics deals with the importance of using objective measurement to

manage security improvements and to steer an information security program. It outlines the best way to design and produce a comprehensive security metrics program. It also describes how to leverage that effort within an organization to achieve improved decision-making, to increase visibility, to perform benchmark comparisons, and to demonstrate the value of the Information Security department[6]. [7] Identifies the disruptions causing vulnerabilities in TBIS. A vulnerability management cycle has been suggested along with many commercial and open source vulnerability management tools. It highlights the importance of resiliency in ERP systems in TBIS. Information security framework of a manufacturing organization has been studied and mapped to the information security framework. [8] Examined to what extent information security metrics are used, how they are used and how organizations benefit from it. This Project contains a background study of existing metrics, an empirical study based on interviews and a discussion and comparison of theoretical procedures and observed practices. [9] Presents a framework for ranking vulnerabilities in a consistent fashion, and some operational metrics used by large enterprises in managing their information systems security process. Assessing the level of information security in an enterprise is a serious challenge for many organizations[10].The provision of security mechanisms in systems is a subset of the systems engineering discipline having a large software-engineering correlation[11].The ERP security framework should ensures that information security forms an integral part of the design, implementation and operation of an ERP system, so the information provided by the system is reliable [12]. Security issues for software systems ultimately concern relationships among social actors stakeholders, system users, potential attackers[13].There must be an economic evaluation of security investment, in order to avoid cost and risks of a security breach[14]. Quantification of information security can be used to obtain evidence to support decision-making about the security performance of software systems[15]. The security of a system should be understood in relation to its environment, in terms of system input and output[20].

3. RESEARCH OBJECTIVE

Businesses are doing more with IT and are more reliant on it, but as the complexity increases, so do the security challenges. So how should a security team determine its security strategy? How much should be spent? What should be prioritized? How to balance between lowering perceived risks and disrupting business? How can a leader, champion and justify decisions to the business?

Security metrics can help an organization to:

- Provide better stewardship via accountability.
- Report progress to business.
- Evaluate exposure and mitigate against damage to reputation.
- Help manage risk effectively
- Demonstrate regulatory compliance.
- Provide justification for security spending.

Measurements provide single, point-in-time views of specific, discrete factors, while metrics are derived by comparing to a predetermined baseline of two or more measurements taken over time. Measurements are generated by counting; metrics are generated from analysis. In other words, measurements are objective raw facts and figures, and metrics are either objective or subjective human interpretations of those data points. Usually, we define information security risk by comparing our assets against perceived threats and vulnerability. But, just like reputation, these elements are often hard to define if not impossible to quantify. Even when defining threat, which is defined as potential to harm, one faces similar challenges. Collecting and analyzing operational metrics needs a well-defined process. With incorporation of reporting/logging functions within most vendor products, this has become less complex than before. The real challenge is how to make sense of this large set of unrelated, heterogeneous security metrics defined by different parts of an organization. It is challenging to make the metrics more meaningful and indicative of unmitigated risks and security control gaps to then be used to support strategic security decisions—thus making it useful to the business. Add to this that security metrics don't have a common defined vocabulary and so many different best practices to follow; one can easily comprehend why metric generation is so difficult.

4. SECURITY METRICS

Security metrics are not about numbers; they are about performance. Unless you have the intestinal fortitude to adequately plan and execute a program to legitimately measure how well specific security programs are delivering on their objectives -- and stand the heat from the answers you may get -- you likely are not going to benefit from this discussion. But your programs will be measured with or without you. Having the answers is just good management. Security metrics for software products provide quantitative measurement for the degree of trustworthiness for software systems[23].Collecting and reporting security metrics is an integral part of an enterprise security strategy[22].Information Security is considered to be an inextricable part of companies' expenditures and there are defined amounts that are invested for its accomplishment, although it is really difficult to determine the best Security Solution[21].Although enterprise information security is acknowledged as one of the most central areas for enterprise IT management, the topic still lacks adequate support for decision making on top-management level[1].

Effective metrics are often referred to as SMART, i.e. specific, measurable, attainable, repeatable, and time-dependent. To be truly useful, metrics should also indicate the degree to which security goals are being met and drive actions taken to improve an organization's overall security program. In the pursuit of metrics that meet these criteria, it is important to consider:

- How difficult collection of accurate data might be for a given metric;
- The potential that the metric might be misinterpreted;
- The need to periodically review metrics that are being tracked and make changes as needed.

From the Literature point of view, asset value, threat, and vulnerability are critical elements of overall risk and are (or should be) weighed in most decisions having to do with security. Each of these elements poses difficulties when trying to incorporate them into a useful security metric. Asset value is the easiest of these three elements to measure; however, certain aspects of value, such as an institution's good reputation, are hard, if not impossible, to quantify. Some believe that threat cannot be measured at all, since it is the potential for harm, although survey results and other information gathered from external sources could be useful in quantifying threat at a high level. Objectively measuring

vulnerability, at least for specific types of networked computer devices, is today relatively easy given the number of quality automated tools to detect levels of computer system vulnerabilities. Measurements of other facets of vulnerability, such as degree of understanding of security issues among computer users, remain somewhat subjective.

Risk = Asset Value x Threat x Vulnerability

Asset Value – easiest to measure ,but difficult to quantify certain assets like institutional reputation .*Threat* – very hard to measure the potential for harm .*Vulnerability* – automated computing device vulnerability tools provide good information, but not all vulnerabilities can be quantified. Regarding potential misinterpretation, consider, for example, the metric often appearing in the popular press that deals with the number of security breaches experienced by a specific entity or industry sector. Many in the security profession would agree that this metric is not necessarily an indication of how secure an organization actually is. Indeed, certain security improvements may reveal security lapses that previously went undetected, and this is a good thing. Although this metric is easy to produce, a security manager should look beyond the institution's security incident record for indicators of security strength and choose metrics that demonstrate true progress toward goals.

Finally, it is important to consider that the effectiveness of a given metric can vary depending upon the maturity of the overall security program and/or specific program component. To illustrate, assume that Enterprise A has just issued a policy that all mobile computing devices must be encrypted and Enterprise B has had such a policy in place for three years. During the first twelve months after policy issuance, Institution A would likely find a metric indicating the level of policy compliance to be very helpful. At Institution B, where device encryption is now routine, allocating resources to track the level of policy compliance would likely no longer be important. The next section discusses this tie between program maturity and effective metrics in further depth.

4.1 Proposed security measures

A vital preparatory step is to evaluate the development of an organization's information security project to confirm the sorts of measures that could be assembled solidly. As a security program develops, its courses of action come to be more institutionalized and repeatable and have a tendency to handle a more amazing amount of information that might be utilized for performance measurement.

• *Implementation measures* are utilized to show advance in executing information security programs, particular security controls, and partnered strategies and methodology. Operational metrics are created from implementation measures and are ordinarily strategic, status-turned, and centered and quantitative in nature with essential gathering of people being security supervisors, security contacts in the products, and product chiefs. Illustration measures are percent of information systems with watchword strategies arranged as needed, percent of apparatuses having corporate arrangement norms, and number of stranded records.

Effectiveness/efficiency measures are utilized to screen if program-level forms and system level security controls are executed accurately, working as expected, and gathering the sought conclusion. These measures address two parts of security control implementation comes about: the heartiness of the effect itself, alluded to as viability, and the convenience of the effect, alluded to as effectiveness. Samples measures are percent of security episodes brought about by shamefully arranged access controls. understandable the effect of information security on an organization's mission or business objectives. Business driven metrics are produced from business impact measures and are regularly key, actionable, far reaching, and explanatory in nature with the essential crowd being senior executives and CISOs. Illustration measures are dollars overspent or under used in information security projects; rundown of discriminating, exceptional or acknowledged dangers; measure of downtime; and take because of strategy violations.

A significant preparatory step is to survey the development of an organization's information security program to figure out the sorts of measures that might be accumulated solidly. As a security program develops, its forms come to be more institutionalized and repeatable and have a tendency to process a more stupendous amount of information that could be utilized for execution estimation. As Figure 2 illustrates, less mature (Stage 1) information security programs need to improve their objectives and goals before having the capacity to execute adequate estimation. Marginally more adult (Stage 2) programs have more described and archived methodologies and use implementation (operational) measures to assess execution. Generally develop (Stage 3 and 4) programs use effectiveness/efficiency and business affect measures to confirm the effect of their information security forms and methodology.

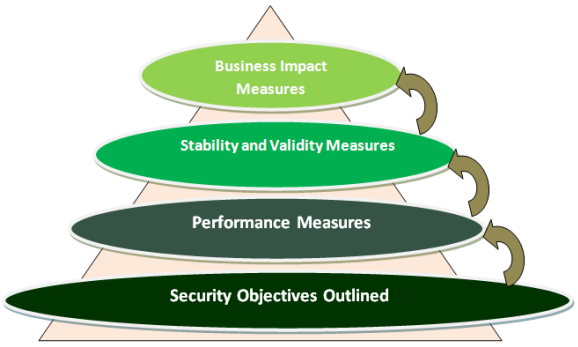

Figure 2. Security Program Maturity and Types of Measurements

A metrics program is closely connected to the maturity level of an organization's information security program.

Stage 1— Describe information security goals and destinations: Then, an organization may as well strive to climb the security development level after some time. To climb the development step, an organization needs to execute on some key exercises.

Stage 2— Outline and arrange: Identify your holdings, define/delegate obligations regarding ensuring those stakes, push information security mindfulness, and define/document a vast hazard administration approach that everyone grasps. In this stage, information security reporting is IT-centered. This is where implementation measures are utilized to show advance in executing information security programs.

Stage 3— Make your methodologies: Integrate information security forms as a part of the organizational security capacity; authorize obligatory security consciousness; institutionalize client distinguishing proof, validation and commission processes/tools; and, institutionalize IT hazard administration with generally outlined danger tolerance and risk/return degrees. In this stage, guarantee that information security reporting is joined to business destinations. This is the place effectiveness/efficiency measures are utilized to screen if program-level forms and system-level security controls are executed effectively.

Stage 4— Completely join with the business: Ensure that information security is a joint authority of business and IT administration with occasional security appraisals that continually assess the adequacy of implementation of the security arrange and formalized episode reaction techniques underpinned via computerized apparatuses. In this level, information security reporting furnishes unanticipated cautioning of updating and rising danger, utilizing mechanized dynamic checking methodologies for all basic systems. This is the place business impact measures are utilized to eloquent the effect of information security on an organization's mission or business objectives.

5. FINDING AND DICUSSIONS

To develop a new security metric program, BIS may as well guarantee the accompanying essentials are set up:

- Strong upper management support
- Practical information security policies and procedures
- Quantifiable performance measures for components
- Disciplined improvement based on analysis.

The ASPIRE approach is to be incorporate for building a great security metrics program for BIS. The area beneath examines each of these steps in the order of execution:

1. **A**im & Objective of the metric program should be defined: Goals of the program ought to be decently characterized and everybody should concur upon the goals in advance. Targets might as well demonstrate abnormal amount activities that must be altogether achieved to meet the objectives. A movement plan ought to be straightforwardly logical from these comments.

2. **S**elect which metrics to generate: Information security metrics might as well attach to the business goals of an organization. Hence, a top-down approach is preferred to a bottom-up approach. Begin this go by distinguishing the structure on which to base your information security metric program then afterward recognize metrics that might show advance to every goal. You are usually more effective with a couple of overall chose metrics. Distinguish the way that your metrics will develop after some time what you measure today may be unique in relation to what you will measure sometime later. Don't only keep tabs on specialized metrics you may as well additionally think about metrics for processes, individuals, client and monetary sways, and risks. When these are carried out, confirm the estimations (certainties and figures) that you'll have to gather for every metric. For instance, a process improvement-based approach would focus on information security processes for which absconds could be discovered and administered. Hence, you have to distinguish those particular information security processes and after that verify estimations for every metric. Interestingly, a compliance-based approach might evaluate how nearly your created information security benchmarks are almost always emulated. In such a case, one should recognize those principles for which consistence ought to be followed and afterward measurements for every metric. So what do you measure? You can effectively get lost when attempting to choose what to begin measuring and investigating. As expressed formerly, the rule to accompany is to begin minor, expand it as time advances, and know when to resign a measure that has ended up unimportant. In your first cycle, keep tabs on territories that measure fundamental information security capacities that help ensure an endeavor. Cases of such measures incorporate influence and administrative consistence, episode taking care of and reaction, helplessness and patch management, arrangement management, and individuals management. In the following process change emphasis, you can then keep tabs on territories that drive information security plans with top management oversight. This may incorporate things, for example identity management, stake management, business prolongation, and debacle recuperation. At last, keep tabs on territories for thorough risk management: chance appraisal remediation, business technique execution, and comparative functions.

3. **P**repare strategies for generating the metrics: These procedures might as well indicate the wellspring of the data, the recurrence of data accumulation, and who is answerable for raw data accuracy, data compilation into measurements, and generation of each metric. This wipes out human failure, brings about better accuracy, and increments benefit.

4. **I**ntroduce measurable performance targets: Counsel industry-particular information assets for potential benchmarks and best practices. Set feasible targets and increase current standards over the long run. Setting targets dependent upon outside principles permits you to analyze your own particular execution and practices against associates inside the industry or "best practice" organizations outside the industry, subsequently making the metric more considerable.

5. **R**eport plan for metric: It is essential to know your gathering of people before you report. The key is to dependably furnish the business connection around the metrics you are providing details regarding. Position, recurrence, conveyance system, and avocation regarding reporting metrics ought to be described in advance, with the goal that the finished item could be imagined at an opportune time by the individuals who will be included in processing the metrics and the individuals who will be utilizing them for decision making.

6. **E**stablish the implementation plan and act, review and refine it: An execution plan might as well hold all undertakings that have to be fulfilled to start the information security measurements program, on top of needed fulfillment dates and assignments. A normal information security measurement usage process has the accompanying four abnormal amount stages:

- The key exercises in the "planning for information gathering" stage incorporate creating a metrics group and determining the metrics and their limits.
- The "source stage" includes discovering the metric source and comprehension its precision.
- The "gather information and investigate results" stage includes change and examination of the raw data.

Mechanization of the gathering is an alternate action in this stage.

- Finally, in the "display and refine" stage we provide details regarding comes about, reexamine metric definitions, distinguish remedial activities, and actualize.

Establish a process to audit and refine periodically check information security metrics guidelines and best practices inside and outside your industry. These aides recognize new advancements and chances to tweak the program. Always validate the accuracy and usefulness of the metrics for the overall information security program and keep track of the processes and resources used to generate the metrics.

6. CASE STUDY

A case study was conducted in a manufacturing industry which processes through information security department. The company was using different standalone software packages for different aspects of business. While this legacy system had served their purposes in the past, the company began to feel that alignment takes time for creating a stronger case for additional security resources and budget allocations.

Our ASPIRE is a holistic, standard-based security measures that guides an organization toward a defense-in-depth approach to managing and mitigating operational risks through the deployment of business information security program. Our ASPIRE security measures makes it easier for organization to establish security program with minimal disruption and distraction.

The company desired insights into their financial and business. So they really needed a system in place to standardize and streamline security metric program and improve operational control through the systems. Metrics is not the focal point for security analytics, but it concretes on how to help business do a better job of aligning security strategy to business priorities on premise software was necessary for definite aspects that required specialized security measures. However there were other aspects where the major need was instantaneous security measures to real time information. The company then uses a ASPIRE measures that would not upset their existing system and would work independently to provide security metrics for BIS.

7. CONCLUSION & FUTURE WORK

Information security metrics can be the key to creating a stronger Business information security program by tracking program efficacy and making the business case for its place in high-level planning. Showing the value of these functions throughout all business processes can also justify strategic security investments. To ensure success, you need to have a plan: Always start small and gradually build on metrics generated in the prior phase. Start by focusing on areas that provide basic information security functions that protect an Business and work up to eventually generating metrics in areas for comprehensive risk management. Be aware of your organization's information security maturity level to understand your limitations and how to progress to the next level. Ensure that you pick metrics meaningful to the business, rather than those that are convenient for IT. Automate where you can. And, always present numbers with analysis in the business context. If you're overwhelmed by the process or don't have the resources to devote to this implementation, consider engaging a trusted IT partner with expertise in information security management. This measured and methodical approach will help you establish a proven tactic to demonstrate program effectiveness—and move you toward a strong justification for information security investment and better business outcomes, now and in the future.

8. REFERENCES

[1] Tashi I., "Security metrics to improve information security management", In Proceedings of the 6th Annual Security Conference, April 11-12, 2007, Las Vegas, NV.

[2] Johansson, Erik.," Assessment of Enterprise Information Security",2010.

[3] Barabanov R., "Information Security Metrics State of the Art", DSV Report series, Mar 25, 2011.

[4] Chaula A and Kowalski S., "security metrics and evaluation of information Systems security", SIDA Sponsored Research Project, 2010.

[5] Swanson M and Bartol N., "Security Metrics guide for Information Technology Systems", Available at: http://csrc.nist.gov/csspab/june13-15/sec-metrics.html

[6] Rathbun D., "Gathering Security Metrics and Reaping the Rewards", October 2009.

[7] Shivani G and Ravi K., "Vulnerability Management for an Enterprise Resource Planning System", International Journal of Computer Applications, Volume 53– No.4, September 2012.

[8] Marte T., "Information Security Metrics An Empirical Study of Current Practice", Specialization Project, Trondheim, December 2012.

[9] Patriciu V and Priescu L., "Security Metrics For Enterprise Information Systems", Journal of Applied Quantitative Methods, Vol.1, 2006.

[10]Johansson,Erik.," Assessment of enterprise information security",EDOC Enterprise Computing Conference, 2005

[11] Vaughn Jr., Rayford B.," Information assurance measures and metrics", International Conference on System sciences ,2012.

[12] Marnewic C., "A Security Framework For An Erp System", International Conference on Information Systems, Dec 2011.

[13]Liu,L.," Security and privacy requirements analysis within a social setting",Requirements Engineering Conference, 2003.

[14] Theodosios Tsiakis.,"The economic approach of information security",2009.

[15] Reijo M. Savola.," Quality of security metrics and measurements", Computers & Security Volume 37, September 2013, Pages 78–90

[16] Patil J., "Information Security Framework: Case Study of A Manufacturing Organization", 2008.

[17]VV Patriciu, I. Priescu, S. Nicolăescu, Security Monitoring - An Advanced Tactic for Network Security Management, Communications 2006 Conference, Bucharest, Romania , 2006

[18]VV Patriciu, I. Priescu, S. Nicolăescu, Operational Security Metrics for Large Networks, International Conference on Computers, Communications & Control (ICCC 2006) - Oradea, Romania, 2012

[19]ISO/IEC. Information Technology - Security Techniques, Code of practice for information security management (final draft), ISO, 2010.

[20] Erland Jonsson and Laleh Pirzadeh.," A framework for security metrics based on operational system attributes", Third International Workshop, 2011.

[21]Theodosios Tsiakis," Information Security Expenditures: a Techno-Economic Analysis"International Journal of Computer Science and Network Security, VOL.10 No.4, April 2010.

[22] Chad Robinson," Collecting Effective Security Metrics" CSO Analyst Reports, 2012.

[23]Juan wang, haowang." Security metrics for software systems", 47th Annual Southeast Regional Conference, 2009.

[24]G. Hinson, "Seven myths about information security metrics," ISSA Journal, Jul. 2010.

[25]D. A. Chapin and S. Akridge, "How can security be measured?" Information Systems Control Journal, 2011.

[26]R. Savola, "A security metrics taxonomization model for software-intensive systems," Journal of Information Processing Systems, Vol. 5, No. 4, 2009, 10 p.

[27]ISO/IEC International Standard 17799:2000 Code of practice for information security management, 2000.

[28]Johnson P., et al., "Using Enterprise Architecture for CIO Decision-Making: On the importance of theory", Proceedings of the 2nd Annual Conference on Systems Engineering Research (CSER), April 15-16, 2004.

[29]Johansson E., et al., "Assessment of EIS - An ATD Definition", Proceedings of the 3rd Annual Conference on Systems Engineering Research (CSER), March 23-25, 2005.

[30] Johansson E., et al., "Assessment of Enterprise Information Security – The Importance of Information Search Cost", Hawaii International Conference on System Sciences (HICSS), January 4-7, 2010.

[31] NIST Special Publication 800-26, "Security Self-Assessment Guide for Information Technology Systems", National Institute of Standards and Technology, 2011.