Managing Information Security Risks:

Understanding and Implementing Effective Security Metrics

(Name)

(Institutional Affiliation)

Abstract

The paper examines select articles pertaining to the security metrics used in information risk management. It begins with a hypothetical case, illustrating the damaging consequences of the utter lack of an information security system vis-à-vis business operations and general standing in the industry. An overview of the information security risk management in general was initially discussed, with subsequent discussions on the varying approaches taken by companies implementing their own security system. The articles delved on the use of security metrics in analyzing existing and potential vulnerabilities of the information management system of a business organisation, defining further security metrics and identifying its ideal characteristics and features to best serve the business interest of a corporate entity. Likewise evaluated are some leading reasons explaining the initial reluctance of most companies in fully implementing security metrics and incorporating the same as equally important components of the business operations.

Toward the end of the paper, an analytical discussion was made on the investment aspect of security metrics and information security, in general, with the end view of making possible recommendations for value managers.

Managing Information Security Risks:

Understanding and Implementing Effective Security Metrics

The increasing complexity of a business operation demands for enhanced information management approach. Concomitant with the need to efficiently manage information for greater efficiency is the need to address potential risks to the security of the information database. The growing reliance on information technology of many business operations calls for a definitive and efficient information security risk management to arrest threats and prevent losses. Take the following sample case highlighting the need for an effective security risk tool:

> A former network administrator at a manufacturing plant thought he had destroyed not only his former employer's manufacturing capabilities but also the evidence that would link him to the crime. The trusted, 11-year employee built and maintained the network at the company. When he fell from corporate grace and knew he was to be fired for performance and behavioral problems, he built a software time bomb to destroy the system.
>
> Three weeks after the network administrator was fired, a plant worker started the day by logging on to central file server. Instead of booting up, a message came on the screen saying an area of the operating system was being fixed. Then the server crashed, and in an instant, all of the plant's 1,000 tolling and manufacturing programs were gone….
>
> ...In the days that followed the crash, the company called in three different people to attempt data recovery. Five days after the crash, the plant manager started shifting workers around the department and shutting down machines that were

> running out of raw materials or creating excess inventory. He took steps to hire a fleet of programmers to start rebuilding some of the 1,000 lost programs.
>
> The company's chief financial officer testified that the software bomb destroyed all the programs and code generators that allowed the company to manufacture 25,000 different products and customize those basic products into as many as 500,000 different designs. The company lost its twin advantages of being able to modify products easily and produce them inexpensively. It lost more than $10 million, forfeited its position in the industry, and eventually had to lay off 80 employees. (Alberts & Dorofee, 2002, pp. 4-5)

Overview of Information Security Risk Management

Managing information security risks is far more than placing firewalls or making backup files of essential programs necessary in various components of the business operation. As Tipton and Krause put it, information security pertains to the "confidentiality, integrity, and availability of information" (2008, p. 16). Information security enables a company to identify specific areas of the business operation dependent on information technology that need protection, sources of threats, the reasons behind the security management system, and extent and duration for as long as such system is needed. Activities dependent on information technology continue to expand. Continuing technological innovations allow for faster exchange of information that correlatively increases the risks and security threats (Killmeyer & Tudor, 2006).

Security Risk Management Tool: Security Metrics

Review of Various Approaches

Different business organisations have variant approaches toward information security threats. In most cases, when a security incident takes place, like a virus infection of a computer unit, companies call in security experts to eradicate the virus while preserving existing files and without compromising computer security in the future (Goetz & Shenoi, 2007). In the long run, however, companies eventually get exasperated addressing countless and specific security invasions.

Most companies lacked long-term goals and specific policies designed to protect information from threats in the future. Reactive approach toward security risks treats security events as mere isolated and manageable incidents. While reactive approach provides a tactical and immediate solution, information system always remains at risk in the future (Wylder, 2004).

Proactive approach takes an entirely different route. Instead of waiting for a security breach to happen, companies with proactive risk management system are able to pre-empt attacks and reduce the vulnerability of the systems from potential threats (Kairab, 2004). A proactive approach necessarily identifies specific business assets prone to security breaches, quantified assessment of damage to the system should a breach takes place, relative financial and operation loss to the company, security vulnerabilities that attackers could exploit, and operation plan to minimise damage to the entire business operations (Purser, 2004).

Defining Security Metrics

Outlining an effective information security risk management system calls for both an objective assessment and analysis of potential prone areas and responses to various threats. Most of quantifiable data are extracted through specific measurements of all pertinent components of information being management. Such measurement alone does not result to the outlining of the specific guidelines companies need to observe; quantitative data still need to be evaluated and analysed. This is the ultimate function of security metrics (Brotby, 2009).

Security metrics, therefore, are the objective analysis and application of all relevant quantitative, statistical, and mathematical information relative to financial costs to the organization, benefits, responses, and requirements necessary to accomplish identified goals (Kovavich & Halibozek, 2005).

Implementing an Operational Security Metrics

Overcoming Management Reluctance

Conventional business tenet dictates that an organisation component should be quantifiable in order to be understood and evaluated by the business top management. The seemingly reluctant reception of business managers in seriously considering security risk management system is largely brought about by the difficulty in quantifying security metrics (Purpura, 2007). Paradigm shift now allows for greater quantification and measurability of security metrics.

Responding to Challenges

Security metrics, designed to inform managers and policy makers in giving a comprehensive and realistic appraisal of the security system, must be able to respond to the demands and challenges of the seemingly new environment. Nichols and Sudbury (2006) gave an outline of the challenges that security metrics need to address. These are as follows:

Establishment of clear objectives. Goals and objective define the direction of the task at hand and provide a baseline for assessment on the effectiveness and efficiency of the security system. Ravenel (2006) clearly understood the need for making a vulnerability and risk assessment as one of the defining guidelines in setting security system goals.

Identification of specific metrics to be used. Consequent to the outlining of the defined goals is the determination of specific metrics that security management needs to use. It entails the use of quantifiable information with the characteristics earlier discussed. Measurability likewise entails the selection of strategies needed for data generation, including manpower requirements, timetable, and presentation (Nemati & Barko, 2003).

Data collection. All information so collected must be processed, analysed, and presented in a manner easily understood by the management who are used to evaluating typical business data and other quantifiable information about the business operation.

Utilization of metric data collected. The ultimate goal is the appropriate use of said data within the proper framework; otherwise, they will only remain in the realm of ideas with practical and essential use in the business operation of the company.

Cost-Benefit Considerations

Investment Considerations

Essentially, putting in place a real working and operational security risk management system entails additional investments. It includes the hiring of additional IT experts and personnel, development of security management software, maintenance cost, and hardware requirements (Vellani, 2006).

At the beginning of the article, a hypothetical security incident was presented, highlighting at the end of the case the actual monetary and financial losses such as loss of standing in the industry and actual loss of revenues due to unrealised orders and expenses incurred in putting in place a reactive security measure (Gupta & Sharman, 2008). Once specific and realistic projections illustrating empirical data on potential loss are included in the presentation, policy makers are likely to understand better the need to put a security structure in place. The end goal, therefore, is a clearer and deeper understanding that designing and implementing an effective and responsive security system is a form of good investment (McCumber, 2005).

Measuring Return of Investment

An essential aspect of the security structure is the quantification of benefits out of the security investment earlier made. Grugescu and Etges (2006) illustrated three main areas justifying making investment in security risk management. These are the following.

Reduced cost or actual gain related to prevention or reduction of information loss. Loss of information through security breaches, damage to essential software utilised in the operation sector of the organisation, and potential exposure to litigations are just some of the situations resulting to actual monetary loss of the company (Rothke, 2005).

Enhancement of operational activities dependent on IT services. The company is able to maximise and enhance existing services of the organisation using information technology. Areas such as database marketing, data gathering, planning, and other operational events will be able to perform better because of significantly reduced or utter lack of security threats to the information system (Calder & von Bon, 2006). Greater efficiency in the performance of various sectors within the corporate setting translates to increased productivity.

Enhancement of the company's overall standing and business performance. Many of them also place equal importance on the manner of delivery and quality of service associated with the business transaction. ISO certifications, for example, illustrate the beneficial effects of putting everything in place with highly efficient operations. Companies known for outstanding service quality, efficient structures, and better technological innovations used translate to better customer service and enhanced standing in the industry.

Comparing and Contrasting Select Information Security Papers

Against the background of what has been earlier discussed is an comparative assessment of three articles written on security metrics and information management in general, namely: *Effective Operational Security Metrics* by J.P. Ravenel, *Implementing Security Metrics Initiatives* by E.A. Nichols and A. Sadbury ; and *Maximizing the Return on Investment of Information Security Programs: Program Governance and Metrics* by C. Grugescu and R. Etges.

A. Finding Common Grounds

All articles are emphatic in emphasising the need to implement a truly effective operations information management security system. The need to outline and design security metrics responsive to the specific needs of a business organisation has been clearly illustrated in all subject articles. Security metrics were distinctly defined, outlining the ideal characteristics and features in order to deliver their stated goals and objectives.

The articles indicate that many companies heavily relying on information management have yet to implement a working and effective security system. They said that most of them only have rudimentary forms of information security systems sans security metrics. All authors succinctly highlight the basic components, purposes, features, and characteristics operational security metrics have and their importance in making an information management system truly operational and responsive to the needs of the business organisation.

Security metrics are designed to provide key information to enable security managers to evaluate the effectiveness and efficiency of their existing security program (Herrmann, 2007). As such, metrics must be able to convey very specific information contained in logical and quantifiable presentation necessary for performance assessment and evaluation. Payne (2006) made a very good and substantial discussion on the nature of security metrics. The primary articles are subject to the comparative evaluation work toward the outlined goals, emphasising the need to reduce, if not eliminate, vulnerable areas of information management system that will eventually translate to greater efficiency, enhanced productivity, and safety of business operations from increasingly eminent security threats.

Survey of Differences

Despite being singular in their emphatic calls for the immediate implementation of an effective security metric system, the articles took slightly varying approaches toward the issue. Ravenel started with a survey made among representative companies concerning their existing information security management system. As illustrated in the article, most favoured simplified and more rudimentary forms of security systems without a more empirical approach toward information security threats. Ravenel likewise gave a more measurable aspect of security metrics with a more defined formula for measuring security risks.

The paper jointly presented by Nichols and Sudbury contains less of those tangible means to measure security risks and the concomitant responses toward their eventual elimination within the information management system of a given business entity. Rather, it was a qualitative discussion of the varying ideal aspects of security metrics. Note, however, that the paper presented by Nichols and Sudbury calls for the implementation of security metrics in managing information security threats. Hence, the paper focused more in outlining the values and challenges that a security metric must address.

Much has been said about the objectives and purposes of an operational security metric system. Potential security gains are measured, and vulnerable areas are identified to minimise security risks to the information system of a business organisation. It remains to be seen, however, if an operational and responsive security system will be incorporated as a basic component of the entire business organisation. Policy makers, especially those in the top management level, remain the ultimate decision makers should a security system be implemented.

The paper jointly presented by Drugescu and Etges addresses this dilemma. Their paper, unlike the previous ones earlier assessed, makes a comprehensive illustration of the investment component of an information security risk management system, incorporating a clearly defined security metrics. Unless a program is presented showcasing potential gains expressed in monetary and other quantifiable terms, top management are less likely to consider the same. The paper is a thorough discussion and guide for security managers to formulate a clear and easily understandable proposal on the implementation of an effective, operational, and responsive information security system.

Conclusion

Good business operations do not only demand for strategic partnership, aggressive public relations, and advertisement and access to clients. Equally important is internal security, especially those pertaining to sectors highly dependent on the information system that are utilised in production lines, manufacturing, information management, data gathering, and other operational services. Paradigm shift now highlights the need for putting in place an effective security risk management system that is effective in warding off security threats and efficient in responding to breaches of security walls both from within and without. Management must be able to understand the essentiality of making the necessary investment for security structures through appropriate presentation of relevant data and other security metrics information. As long as there are defined and feasible goals outlined in the context of actual and potential needs of the organisation, security metrics and the eventual security structure in place will be able to protect the business operation from the increasingly growing threats posed by high dependability on information technology.

Recommendation

It has been clearly shown that security metrics form part of the key component of the security system designed to protect valuable information and increase productivity and efficiency of the organisation. At the onset, value managers need to shift their approach toward information management. Reluctance amongst policy makers in seriously considering the full use of security metrics should be overcome. It should be always viewed as a challenge if one is sentient of the critical role security metrics play in the business environment.

Management people must shift paradigm and take a closer and more serious look at security metrics, not just as an option or enhancement to whatever existing information management system the company has. Security metrics must be understood as vital components of the said system.

Managers tasked to handle information security system must be able to clearly identify specific features of the security metrics and re-design the same in the context of an existing information management system. There is greater need and urgency to use one should there be no existing security system at all. Since top managers are used to interpreting and evaluating any business proposal in terms of investment cost and monetary gains, i.e., numerical figures, a proponent must, therefore, design a presentation on the proposal for the security metrics in a manner easily understood and appraised by the management. The presentation must not be limited to a seemingly abstract illustration of the features and objectives of the security metrics. Rather, the proposal must be expressed in easily quantifiable manner. Implementing an operational and truly effective security measure demands substantial investment necessary for the formation of the technical personnel, acquisition of software and hardware, periodic operations, and maintenance of the entire system. As such, all benefits that are projected to redound to the company must be presented as empirical returns of investment and not just as a theoretical elucidation on security metrics.

References

Alberts, C. J., & Dorofee, A. J. (2002), *Managing information security risks: The OCTAVE approach*. Boston: Addison-Wesley.

Brotby, W. K. (2009). *Information security metrics: A definitive guide to effective security monitoring and measurement*. Florida: CRC Press.

Calder, A., & von Bon, J. (2006). *Implementing information security based on ISO 27001/ISO 17799: A management guide*. Texas: Van Haren Publishing.

Goetz, E., & Shenoi, S. (2007). *Critical infrastructure protection*. New York: Springer.

Gupta, M., & Sharman, R. (2008). *Handbook of research on social and organization liabilities in information security*. London: Idea Group, Inc.

Herrmann, D. S. (2007). *Complete guide to security and privacy metrics: Measuring regulatory compliance, operational resilience, and ROI*. Florida: CRC Press.

Kairab, S. (2004). *A practical guide to security assessments*. Florida: CRC Press.

Killmeyer, J., & Tudor, J. K. (2006). *Information security architecture: An integrated approach to security in the organization*. Florida: CRC Press.

Kovavich, G. L., & Halibozek, E. P. (2005). *Security metrics management: How to measure the costs and benefits of security*. Massachusetts: Butterworth-Heinemann.

McCumber, J. (2005). *Assessing and managing security risk in IT systems: A structure methodology*. Florida: CRC Press.

Nemati, H. R., & Barko, C. D. (2003). *Organization data mining: Leveraging enterprise data resources for optimal performance*. London: Idea Group, Inc.

Nichols, E. A., & Sudbury, A. (2006). Implementing Security Metrics Initiatives. Retrieved June 29, 2010, from http://infosectoday.com/Articles/Nichols.pdf

Payne, S. C. (2006). A Guide to Security Metrics. Retrieved June 29, 2010, from http://www.sans.org/reading_room/whitepapers/auditing/guide-security-metrics_55

Purpura, P. P. (2007). *Security and loss prevention: An introduction*. Massachusetts: Butterworth-Heinemann.

Purser, S. (2004). *A practical guide to managing information security*. Massachusetts: Artech House.

Ravenel, J. P. (2006). Effective Operational Security Metrics. Retrieved June 29, 2010, from http://www.issa.org/Library/Journals/2006/February/Ravenel%20-%20Effective%20Operational%20Security%20Metrics.pdf

Rothke, B. (2005). *Computer security: 20 things every employee should know*. New York: McGraw Hills Professional.

Tipton, H. F., & Krause, M. (2008). *Information security management handbook*. Florida: CRC Press.

Vellani, K. H. (2006). *Strategic security management: A risk assessment guide for decision makers*. Oxford: Butterworth-Heinemann.

Wylder, J. (2004). *Strategic information security*. Florida: CRC Press.