INFORMATION SECURITY RISK MANAGEMENT

[1]Usha, [2] Ankush Goyal

[1,2]Computer Science & Engineering Department, M.D.U, (India)

ABSTRACT

Optimizing risk to information to protect the enterprise as well as to satisfy government and industry mandates is a core function of most information security departments. Risk management is the discipline that is focused on assessing, mitigating, monitoring a optimizing risks to information. Risk assessments and analyses are critical sub-processes within risk management and are used to generate data that drive organizational decisions to accomplish this objective

Keywords*: *Risk Management, Security, Vendor, Introduction, Impact

I. INTRODUCTION

Information risk management is the activity directed towards assessing, mitigating (to an acceptable level) and monitoring of risks associated with information. The principle goal of an organization's risk management process should be to protect the organization and its ability to perform their mission, not just its IT assets [70]. Peter Drucker once said "the diffusion of technology and commoditization of information transforms it into a resource equal in importance to the traditionally important resources of land, labor and capital" [14]. The exponential growth and availability of information after the Internet boom of 1990's goes to show the accuracy of his foresight. In today's world, the fortunes of most organizations are tied with the information they possess and the sophistication with which they are able to manage it. Most of these risk management methodologies, while providing a structured and systematic process for risk management, either lack specific guidance on which risk assessment methods to use or provide for a weak approach. This does not satisfy the rigorous data needs of business leaders as well as audit needs of compliance auditors. This was clearly identified as a significant issue in the recent RSA report based on discussions with top risk management leaders in Global 1000 companies [61]: "Risk should be managed to an acceptable level, based on the enterprise's risk appetite with decision-making guided by a risk assessment model. A structured, consistent and repeatable process for making the risk/reward calculation helps to ensure that it is done consistently across the organization".

II. CHARACTERSTICS IN METHODOLOGY IN RISK MANAGEMENT

A comprehensive definition of the characteristics desired from a risk management system in one place is missing from current literature on this topic. We propose the following criteria based on our research (these criteria are articulated in our paper [64]):

1. It must manage risks to an acceptable level based on enterprise's risk appetite [61]. 2. It must provide decision-support [61]. Security investments are expensive and risk is one criterion that is used to address the economics around it.

3. It must be a continual process [35]. Risk management is not conducted at a point in time; it should be considered throughout the lifecycle of systems development.

4. It must be aligned with an organization's business objectives [70].

As the amount as well as complexity of information resources within organizations is increasing at an exponential rate, we also consider the following characteristics as desirable traits: 5. It must be adaptive. Since an organization's risk profile, threats and vulnerabilities change frequently, it is important that risk management should be adaptive to these changes.

6. It must be scalable to accommodate for this increasing complexity while not impacting the window desired to conduct the assessment activities.

7. It must ensure compliance with government and industry mandates.

8. It must produce consistent results irrespective of who conducts the responsibilities associated with risk management

III. IMPACT OF SECURITY ENHANCEMENT

Based on the risk assessment analytics, a risk assessor provides recommendation on how controls need to be adjusted or whether new controls need to be added. However, decision makers want to measure the impact of these security enhancements. For e.g. increasing the strictness of configuration of a control might mean that the end user sees increased response times; for a decision maker, it is critical to understand whether increasing that strictness and the inconvenience caused to the end user as a result is worth it or not in terms of prevention of security threats. While this area has been researched in other disciplines such as microprocessor simulation [78], it remains unaddressed within the domain of information security.

IV. SECURITY THREATS

The risk profile of an organization changes on a very dynamic basis because new threats come into existence on an almost continuous basis. Thus any approaches to deal with the threats have to be dynamic as well. This issue has not been dealt with in existing research, either methodologically or architecturally. One essential aspect of being able to manage the information security risk to the enterprise is configuring security controls appropriately to ensure that the organization is protected against the threats impacting it. However, despite this critical need, there is a significant opportunity in current approaches that are used for this purpose. They are initially configured during the installation phase and then changed only on an event driven basis. These events could be things like an incident, or observation from logs or recommendations from a risk assessment exercise. There are significant issues with this approach: these changes are ad-hoc and either happen after the fact (i.e. the loss to the enterprise has already happened at that point) or are not dynamic in nature (it makes sense to manage security configuration as soon as the security controls start sensing that the nature of threats around it has started changing).

V. VENDOR SECURITY

A policy is typically a high level articulation of management's intent. As such, it does not provide more granular direction and measurable metrics, which would make the task of adhering to it easier for rest of the enterprise. [25] demonstrates the effective way of writing security policies. Standards are used for this purpose. A standard is refinement of the policy to a more granular level and provides the requirements that need to be met for adherence to the policy. Figure 5.3.2 shows a sample vendor information security standard. It is based on the controls

and control objectives provided by ISO 27001 [36]. This standard can be used as a starting point if one doesn't exist already for the enterprise. Note that just the creation of policy and standard is not going to be sufficient unless it is followed up by extensive propagation through the enterprise. This needs to be accomplished through training. Our recommendation is to make it mandatory for all key stakeholders.

VI. CONCLUSION

A survey of current literature as well as prevalent risk management practices in enterprise environments indicates that there are some significant limitations in current risk management approaches. Although control selection and management is a crucial part of risk assessment process of these methodologies, no formalized methods exist that help manage these aspects. In addition, the area of managing risks due to vendors of the enterprise as well as a requirements engineering framework for determining an appropriate GRC strategy remain unaddressed as well.:

VII. ACKNOWLEDGMENT

I show my thanks to all the departments' personals and sponsors who give us an opportunity to present and express my paper on this level. We wish to place on my record my deep sense of gratitude to all reference papers authors for them valuable help through their papers, books, websites etc.

REFERENCES

[1]. R. Anderson, "Why Information Security is Hard- An EconomicPerspective", 17th Annual Computer Security ApplicationsConference, Dec. 2001.

[2]. Jonathan D. Andrews, "Erosion of Trust - E-commerce and theLoss of Privacy", Information Systems Control Journal, Vol. 3, 2001, pp. 46-49.

[3]. Georges Ataya,"Risk-aware Decision Making for New ITInvestment", Information Systems Control Journal, Vol. 2, 2003, pp. 12-14.

[4]. Rudy Bakalov,"Risk Management Strategies for OffshoreApplications and Systems Development", Information Systems Control Journal, Vo. 5, 2004, pp. 36-38.

[5]. S. P. Bennett and M. P. Kailay, "An application of qualitative risk analysis to computer security for the commercial sector", Eighth Annual IEEE ComputerSecurity Applications Conference, Nov.-4Dec. 1992, pp.64-73.

[6]. Nicholas A. Benvenuto & David Brand, "Outsourcing: A RiskManagement Perspective", Information Systems Control Journal,Vol. 5, 2005, pp. 35-40.

[7]. B. Blakley, E. McDermott and D. Geer, "Information Security isInformation Risk Management", Proceedings of the2001workshop on New security paradigms, 2001, pp. 97-104.

[8]. PaulBrooke,"RiskAssessmentStrategies",NetworkComputing,30thofOctober,(http://www.networkcomputing.com/1121/1121f32.html?ls=NCJ_1121bt).

[9]. S. A. Butler,"Security Attribute Evaluconference on Software engineering, ACM, May 2002, pp. 232-240.

[10]. K. Campbell, L. A. Gordon, M. P. Loeb and L. Zhou, "The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market", Journal of

Computer Security, Vol. 11, 2003, pp. 431-448.

[11]. H. Cavusoglu, B. Mishra and S. Raghunthan,"The Effect of Internet Security Breach Announcements on Market Value of Breached Firms and Internet Security Developers", International Journal of Electronic Commerce, Volume 9, Issue 1, 2004, pp. 70-104.

[12]. F. Cohen, "A Cost Analysis of Typical Computer Viruses andDefenses", Computers & Security, Vol. 10, 1991, pp. 239-250.

[13]. Center for Internet Security (http://www.cis.org)

[14]. Drucker, Peter, 1988. 'The Coming of New Organization', HarvardBusiness Review.

[15]. Peter Drucker,"The Practice of Management", Butterworth-Heinemann, 2007.

[16]. CriminalTake ControlofCheckFree Web Site(http://pcworld.about.com/od/networkin1/Criminals-Take-Control-of-Chec.htm)

[17]. COBIT 4.1, ISACA (http://www.isaca.org/).

a. Enterprises Risk Managemen Integrated Framework(http://www.coso.org/).

[18]. Covington, Prahlad Fogla, Zhiyuan Zhan, and Mustaque Ahamad. A context aware secur A context aware security architecture for emerging applications. In Proceedings of 18th Annual Computer Security Applications Conference (ACSAC), pages 249-258, as Vegas, NV, December 2002.

[19]. Risk Management: Implementation principles and Inventories forRisk Management/Risk Assessment methods and tools, European Network and Information Security Services.

[20]. G. Eschellbeck,"Active Security- A Proactive Approach for Computer Security Systems, Journal of Network and Computer Applications, No. 23, 2000, pp.109-130.

[21]. F. Farahmand, W. J. Malik, S. B. Navathe and P. H. Enslow,"Security Tailored to the Needs of Business", Proceeding of theACM CCS BIZSEC, October 2003.

[22]. F. Farahmand, S. B. Navathe and P. H. Enslow, Electronic Commerce and Security A Management Perspective, ISS/INFORMS Seventh Annual Conference on Information Systems and Technology, San Jose, 2002.

a. Shared Assessments, http://www.sharedassessments.org.

[23]. Todd Fitzgerald,"Ten Steps to Effective Web-Based Security Policy Development and Distribution", in Information Security Handbook, Harold Tipton and Mickey Krause Eds., Auerbach Publications, Boca Raton, FL, 2005.

[24]. Todd Fitzgerald,"Building Management Commitment Through Security Councils", Information Systems Security, May/June 2005.

[25]. D. E. Geer, "Making Choices to Show ROI", Secure Business Quarterly, Vol. 1, Issue 2, 2001, pp. 1-3.
K. Ghosh and T. M. Swaminatha, Software Security and Privacy Risks in Mobile E-Commerce, Communications of the ACM, Feb.2001, Vol. 44, No. 2, pp. 51-57.

[26]. L. A. Gordon and M. P. Loeb, "Return on Information Security Investments", Strategic Finance, Nov. 2002.

[27]. John Hagerty,"The Governance, Risk Ma Risk Management, and Compliance Spending Report, 2008-2009: Inside the $32B GRC Market", http://www.amrresearch.com.