Survey of Information Security Risk Management Models

Derek Mohammed
School of Business
Saint Leo University
Florida USA

Shereeza Mohammed
School of Education
Walden University
Minnesota, USA

Abstract

Information security in a current and urgent issue for government and industry with the increasing frequency of cyber security breaches that have occurred in terms of hacking and information theft. To address such issues several approaches have been and continue to be devised to keep abreast with the advances in technology and the skills of those intending harm. To manage the risk inherent in information security several strategies and frameworks are explored. There have been three generations of security risk management strategies as well as governing standards and processes that have been put into place with varying success. Additionally, three security risk management frameworks are analyzed in terms of their effectiveness, policy and legislative relevance and alignment to security and control processes.

Keywords: risk, information security, data protection, risk management framework, risk assessment

1. *Introduction*

In today's fast paced technological age, computer technology and information dissemination are essentially ubiquitous as are instances of cyber security attacks, hacking, and information theft. From its earliest inception as a strictly technical initiative to combat risks and threats to a system or network and to safeguard the integrity, availability, and confidentiality of data, the concept of Information Security (IS) management has evolved into an all-encompassing effort to protect and facilitate the "controlled sharing of information and managing the associated risks across a changing threat environment" (Chukwuna and Rai, 2010), and has become an embedded function in business organizations.

In the 1990s, the British Standard (BS 7799) sought to set domestic information security management standards for users, data, and processes within the United States (Pan et al., 2010). Since then associated threats to security has kept pace with technology advances. In 2000, the Consortium for Research on Information Security and Policy (CRISP) initiated a comprehensive study to explore the multi-dimensional aspects of the international information security risk problems and to formulate strategies to address the legal ramifications; examine the intra- and inter-corporate policies affecting security information protection and risk; determine the existence of legislation affecting domestic and international governmental policies; as well as to identify the existing technological security constraints and to brainstorm for futuristic technological infrastructure improvements or innovations that would be required to meet and satisfy the ever-changing needs of the global technological society.

From the outset, it was clear that an integrated approach that spans across language, international, and cultural borders was the only viable and lasting solution. At the core of each of these discussion areas of safeguarding computer infrastructure was the establishment of an internationally derived constituency of stakeholders to formulate specific, implementable strategies to foster global cooperation among governments, businesses, academicians, technology users, and technology innovators and engineers. Within the Information Systems Security sector (InfoSec), information assurance professionals have been tasked with developing and then implementing sound information and network security risk assessments as well as risk management programs.

2. *Generations of Security Risk Management Strategies*

To date, no less than three evolutions or generational approaches have been used to address security risk management strategies. The originators of the first generation security risk protocols developed technical tools and used non-quantitative methods to address security issues. The Second generation approaches were improvements but were viewed as temporary fixes. The third generation, however, used quantitative decision analysis and explicitly incorporated uncertainty and flexibility through data collection, data standardization, and data sharing to provide measures of relevance, standardized terminology, and associated liability (Soo Hoo, 2000).

Presently, the International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC) provides one of the most comprehensive and accepted information security risk standards, namely ISO/IEC 27002. A national certification in ISO/IEC 27001 standards is available and over five thousand organizations have gained that certification. Many countries such as Great Britain, New Zealand, and Australia have instituted their own national standards. Popular security risk management publications and methodologies include COBIT, NIST Special Publication 800-30, CRAMM, and Factor Analysis of Information Risk or FAIR (Rot, 2009).

According to Saleh et al. (2011), security risk management is a multiple step process: assessing security management risks, and defining a security risk management framework. The first step in a viable security risk management process is assessment. While safeguarding computer networks and information is a high priority goal, in the past, security risk management strategies or so-called "fixes" have focused on only one or two areas. Instead, an integrated approach should be used which addresses three key risk assessment aspects, which include: the preservation or protection of data; the system vulnerabilities inherent in the information security framework; and the presence of insider threats. Soo Hoo (2000) proposed that the security risk associated with the preservation of protection of data was an amalgamation of four factors: data integrity, availability, authenticity, and confidentiality. Data integrity is most closely identified with readability and completeness of baseline information while data availability implies simple access. Authenticity is directly related to data validity and possessing genuine, verifiable information from trusted sources. Lastly, confidentiality entails limiting disclosure and observation of data to authorized users.

System vulnerabilities are two-fold. First, faults and weaknesses can be inherent in or a part of the overall system network; therefore, risk assessment and corresponding mitigation plans must be devised to implement appropriate built-in and attack response and protection measures. Additionally, system vulnerabilities and associated risks may be due to natural disasters. Despite one's best efforts, these threats cannot be averted, but their effects can be mitigated with comprehensive planning. For example, in 2004, the Small Business Administration boldly announced that all fifty states would experience a major natural disaster by the year 2006 from either a flood, mudslide, wildfire, tornado, hurricane, tsunami, volcanic eruption, or earthquake (Weinberger, 2004). Two years later, in 2006, information technology (IT) executives ranked natural disasters as the third greatest threat to an overall information system.

Humphreys' (2008) research on the other hand, focuses on the sources of security management risks from insider threats, lack of due diligence on safeguards being mandated by key executives and board members, and, lastly, insider vulnerabilities. First, insider threats can arise from any number of employee or on-site contractor sources. Pay grade has no bearing on the likelihood of being a security threat, and insider threats account for 35% of international security theft and sabotage incidents. For these perpetrators, it is more about their personal motive or dissatisfaction that can arise from various estrangements or intentional illegal acts of greed displayed by rogue, or disgruntled employees (Farkus and Jojodia, 2002). Per record, average security breech costs can range from a low of $90 to $305 and includes legal fees, lost productivity, government fines, customer restitution, and public relations fixes, as well as the immeasurable cost of undermining public perception and confidence. Who is most likely to create a security risk? Anyone including the board of directors, staff and paid contractors can exploit the vulnerabilities of an existing system to gain access to and then profit from confidential information. Further, all these stakeholders also have the potential to maliciously sabotage or damage data, software, or hardware.

The second insider threat, the lack of due diligence, is generally not due to malicious intent. To the contrary, it signals that key executives and board members do not comprehend the importance of establishing, monitoring, and then assessing security risk protocols and taking a top-down approach to relaying security priorities to subordinates. The third threat involves insider vulnerability.

Also called "human challenge" this threat frequently adds to the breadth of security management risks. This presents an organizational challenge that encompasses both the work role of an individual as well as the employee's personal beliefs, attitudes, norms, mores, and perspectives. These human challenges include mistakes in judgment, errors in data handling, carelessness, and the lack of employee training. Such human-related challenges, often complicate and threaten organizational data and hardware assets (Ashenden, 2008).

3. *Defining a Security Risk Management Framework*

There is certainly no shortage of suggestions within the IT Security profession regarding how to design a Risk Management Framework. The following section discusses the National Infrastructure Protection Plan advocated by Saleh et al. (2011), a Risk Profiling schema by Atyam (2010), and the User Participation-Sarbanes Oxley approach authored by Spears and Barki(2010). Saleh et al. (2011) suggest a security risk based framework should center on a national infrastructure protection plan (NIPP) which is designed to enhance continuous process improvement efforts which, when implemented, will afford critical protection to resources and infrastructure. This framework is built upon a four step process: assessment of system risks, implementation and maintenance of a security framework, monitoring activities, and a final review and improvement process. At its core, the NIPP risk management framework prioritizes risks and then implements a proactive security risk protocol to address problems.

Framework effectiveness is tested using the network risk management software, SpiceWorks. This software is designed to integrate network management applications, a help center, and computer inventory tools as well as provide detailed scans of Windows, Linux, or Mac devices. The protocol is part of an overall information security cultural framework in which information security has a direct impact on information security user behavior. Positive user behavior, then, is able to cultivate a positive information security cultural environment.

Atyam (2010) suggests a different process based on customer requirements and needs through risk profiling. To this end, he advocates the use of a business operation (FORTRESS) and technology solution application (FAÇADE) for profiling purposes. A company's needs center on recognized security gaps in a business's security controls. Atyam (2010) separates these gaps into Type I and Type II and his research focuses on the various risk profiles which emerge from the Types I and II security gaps. Type I gaps stem from understanding the technology solutions used and the rationale behind the use of information and its data for interfacing and enabling a solution provider. On the other hand, Type II gaps arise from exploitable technology vulnerabilities within the system and how these system vulnerabilities negatively affect reliance on a proposed security risk solution. This research on risk profiling determines that data security is most often compromised by access control, IT continuity management, and network access controls. Risk profiling suggests that information exchange, compliance, asset management, and antivirus software use are the least likely to be serious control risk assessments. Atyam(2010) states that the "business impact can be determined upon assessment of the vulnerabilities and probability of threat exploiting the identified vulnerabilities" and these measures can be expressed as high, medium, or low vulnerabilities within an organization. This research recommends that an effective framework should center on password management, segregation of duties, proper system configuration, authorized user connectivity and user profiles, identified log on protocols, and the isolation of sensitive data. Once this framework is in place, the servers and network can be tested through various vulnerability assessments. Initial results provide a business baseline for investigation and improvement.

A third model developed by Spears and Barki(2010) uses a governmental construct, the Sarbanes-Oxley Act (SOX) as a methodology to test a framework based on user participation. Because federal oversight of business practices was increased under Sarbanes-Oxley, this research investigates the link or causality between security risk management and levels of government regulatory mandates. At its core, SOX links integrity of business information and financial statements to internal control. Since financial and business information is housed and accessed through computer information systems, the government has a vested interest in protecting the integrity of the information from mistakes, sabotage, data theft, and other outside security threats. The researchers believe that linking SOX to a framework for security risk management is important for two reasons. First computer information and data entry have a direct impact on the final result of financial statements that must be approved by key executives as to its accuracy. Secondly, the technical controls established by a company affect the internal and external threats to data security and security risk management.

4. *Analysis of Models*

Saleh et al's(2011) research focuses on the results of the testing of a specific software, Spice Works. Through their profiling technique, Saleh et al. (2011) were able to isolate major security risk events as failures, warnings, and errors. Total failures of the security system have a low rate of occurrence and reoccurrence. On the other hand, warnings and errors are frequent and have a high likelihood of occurrence and reoccurrence.

The most critical issues are service control manager and server warnings as well as net runtime and system service module installation problems. Since the assessment process is highly interactive among its assessment areas, the risk assessment framework is considered to be highly effective. Saleh et al. (2011) suggest that frequent warnings and errors in the security system pose a bigger threat that is capable of transforming into real system issues and system vulnerabilities. The framework assessment points to priority areas of security risk and concern. It is management's responsibility to define a degree of acceptable risk and, if needed, to supplement the system and infrastructure with additional resources.

Atyam's (2011) research results are largely anecdotal. He can point to successes in identifying problem areas in security risk management, but his study was limited to retail businesses and banks. His focus seems to be the identification of risks to control, not in the engineering of an actual solution. As a result of their user participation research and security risk management frameworks, Spears and Barki(2010) proposed that user participation affords greater organizational awareness, improvement of security control performance measures, and increased levels of business environmental alignment with security and control processes.

5. Conclusion

As businesses increase their international presence in the global economy, reliance on timely, accurate, and reliable data will only become more important. Assaults or attacks against data will only increase, therefore, security risk management protocols must be put in place or developed to meet increased security challenges and needs. No one approach is sufficient. An integrated approach, using risk assessment tools, identifying insider and external risks, and developing a corresponding, but flexible, framework to ferret out these security risks and vulnerabilities will be needed. Businesses must act in concert with governmental or regulatory bodies to design legislation protecting data, to craft appropriate integrity policies and reliance standards, and fostering unique ways to promote technological advances in information data security and security risk management solutions.

References

Ashenden, D. (2008). Information security management: A human challenge? *Information Security Technical Report, 13* (4), 195-201.

Atyam, S. (2010). Effectiveness of security control risk for enterprises: Assess on the business perspective of security risks. *Information Security Journal: A Global Perspective, 19*(6), 343-350.

Chukwuma, P., &Rai, S. (2010). Top 10 Security and Privacy Topics for IT Auditors. *Information Systems Audit and Control Association Journal, 2*.

Farkus, C.,&Jojodia, S. (2002). The inference problem: A survey. *ACM Special Interest Group on Knowledge Discovery and Data Mining, 4* (2), 6-11.

Humphreys, E. (2008). Information security management standards: Compliance, governance and risk management. *Information Security Technical Report, 13* (4), 247- 255.

Pan, Y., Stackpole, B., &Troell, L. (2010). Computer Forensics Technologies for Personally Identifiable Information Detection and Audits. *Information Systems Audit and Control Association Journal, 2*.

Rot, A. (2009). Enterprise information technology security: Risk management perspective.

Proceedings of the World Congress on Engineering and Computer Science, San Francisco, California, USA.

Saleh, Z., Refai, H., &Mashhour, A. (2011). Proposed framework for security risk assessment. *Journal of Information Security*, 2, 85-90.

Soo Hoo, K. (2000). How much is enough? A risk-management approach to computer security. Retrieved fromhttp://cisac.fsi.stanford.edu/sites/default/files/soohoo.pdf

Spears, J. & Barki, H. (2010). User participation in information systems security risk management. *MIS Quarterly, 34* (3), 503-520.

Weinberger, J. (2004). Averting customer data loss. *CRM Magazine, 8* (10), 16.