Analysis of the federal information security management act (fisma) essay sample

Law, Security

Foreign as well as domestic cyber threats and attacks on technological networks and systems have led the Government to enact the Federal Information Security Management Act (FISMA), which is a section of the E-Government Act of 2002. FISMA provides the statutory structure required for management, reporting, assessment and compliance. This paper will provide an analysis of FISMA and why compliance under the Act while need, is more taxing and less security.

“ This paper or presentation is my own work. Any assistance I received in its preparation is acknowledged within the paper or presentation, in accordance with academic practice. If I used data, ideas, words, diagrams, pictures, or other information from any source, I have cited the sources fully and completely in footnotes and bibliography entries. This includes sources which I have quoted or paraphrased. Furthermore, I certify that this paper or presentation was prepared by me specifically for this class and has not been submitted, in whole or in part, to any other class in this University or elsewhere, or used for any purpose other than satisfying the requirements of this class, except that I am allowed to submit the paper or presentation to a professional publication, peer reviewed journal, or professional conference. In adding my name following the word ‘ Signature’, I intend that this certification will have the same authority and authenticity as a document executed with my hand-written signature.

Introduction

What is FISMA?

As the largest employer in the United States (“ US”), the Federal

Government (“ Government”) is tasked with providing service to the public as mandated in the United States Constitution (U. S. Department of Labor, 2011). In trying to fulfill this audacious task, it is only sensible and fitting that the Government take steps in a technology driven world to protect its information infrastructure, network, systems and services. Therefore in 2002, the Federal Information Security Management Act (“ FISMA” or “ Act”) was established (McDonald, 2010). Purpose

FISMA’s sole purpose is to protect the Government’s information by providing a “ comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Government operations or assets” for (Cornell University Law School, n. d, p. 1). Literature Search

The literary research performed involved utilizing online search engines like Google, Yahoo, and Bing by inputting keywords, phrases and Boolean terms. Additionally, I used online links provided in the webtyco classroom to find whitepapers and other articles. Analysis

In researching and analyzing FISMA, the basic scheme can be broken down into four key components: 1) Requirements, 2) Compliance, 3) Risk assessment, and my favorite component 4) Cost (Rasmussen, 2010). Requirements

FISMA necessitates compliance for all data and information systems, under the governments control and all data and systems that are provided by others outside the public domain (GovITWiki, 2008). Data that is provided by

others to governmental agencies must strive to protect those systems operations, and assets, and provide continuity in system reporting and other requirements (IBM, 2007). Agencies must produce a total, accurate, and complete assessment of all information and systems including security status, risk, and remediation (IBM, 2007). However, this can be very taxing when systems are " spread across many organizations and geographies" (IBM, 2007, 4.) FISMA mandates basic security standards and requirements by putting the onus of complying with these requirements on each agency to detect and report security vulnerabilities in computer systems (Hasson, 2008). Additionally, these requirements to mandate security standards are ongoing with reporting requirements that are provided at least annually if not more to OMB who must submit yearly reports to Congress on agency compliance and outcomes (Hasson, 2008). This reporting requirement already exist in the Government , but the Act just added the need to secure information systems as well as information which I think is a nature progression in a technological environment (Hasson, 2008).

Compliance/Challenges

With every Compliance requirement established by FISMA, there is the challenge of each agency to produce the desired effect of such requirements (TechTarget, n. d.). Under the thumb of the National Institute of Standards and Technology (NIST), nine steps have been identified as a gauge agencies should strive towards in order to be in compliance (TechTarget, n. d.). These steps are protecting information, control of information, risk assessment, documentation of controls used to devise a system security plan,

implementation of security controls, assessment of security controls once online and in use, risk to the agency and its mission, process authorization and continuous monitoring of security mechanisms (TechTarget, n. d.).

For instance, under FISMA Government agencies must make sure all public information and systems housed in the agency are free from alteration and manipulation, and maintained in a manner that protects information against malicious threats and/or inside attacks all in a cost effective way (IBM, 2007). This is no doubt very difficult for agencies trying to focus on securing data while also being required to worry more about meeting multiple compliance standards (IBM, 2007). The growing census in the public sector is that FISMA doesn't really address if the implementations reported by agencies really secure data and systems because the focus is on the reporting/compliance and not security (Hasson, 2008). Moreover, annual reviews of agency's information security programs and reports are provided per the Act to OMB who reports to Congress; however Is yearly reporting really enough? or should system checks take place quarterly or even monthly? The Act doesn't address why annual reporting is the rule of thumb and it should (Hasson, 2008). Risk

At the heart of any compliance or reporting requirement is the Risk Factor meaning " How much risk exists and since it cannot ever be prevented ' How can it be minimized, tracked and predicted?" The answer is by knowing what data and systems one must protect, what it takes to protect the data and systems, and what is the most strategic and ongoing means of testing and tracking systems (Collmann, 2007). Moreover, what methods should be used

to see if an attack can be anticipated or weaknesses and vulnerabilities exploited (Collmann, 2007). The best methods for achieving these goals are to 1) know what data and systems you have and who uses them 2) know how often the systems are used and have detection methods in place that will discover any anomalies in data/system access (National Institute of Health, 2009). The Act addresses these issues and requires remediation as a means of answering these questions (IBM, 2007). However, systems change and technology improves and changes and the Act must address and account for such changes (Hasson, 2008). Cost

With every Act there is of course the question, " Who Will Pay?" In this Act, FISMA is somewhat silent on this issue. One can only surmise that the Government (i. e. Joe Citizen's taxes) will be responsible for all compliance/reporting requirements, implementation, and continual risk assessment (Rasmussen, 2010). The Act does discuss performance as a requirement or budgetary item (Hasson, 2008). As long as agencies are getting high performance rating for compliance and improved or stellar security measures, their budgets will be adequately funded (Hasson, 2008).

However, reporting, compliance and other factors place additional burdens on agencies that weren't as voluminous before; this mandate will cause agencies to achieve optimal compliance, but inadequate security (Hasson, 2008). This method of compliance is analogous to standardize test taking methods. Teachers teach to children with the desire for them to past test so their school will be adequately funded and not so the children can learn, which is the whole point. With all the compliance requirements mandated

within the Act, how can cost effective measures be implemented? Well, the Government already operates under several reporting requirements that are in line with the Act's requirements and all FISMA needs to do is expound and broaden the scope of these requirements (Rasmussen, 2010). Therefore, a more streamlined approach should be designed to use present requirements with past policy thereby allowing for a more efficient and cost effective statutory scheme (IBM, 2007).

Conclusion

Overall, the Government is moving in the right direction in trying to protect public information and information systems from exploitation. However, the reporting requirements need to overhaul. The Act as written is too stringent, and laden with numerous compliance requirements that may cause more harm than good. Maintaining the Act's true mission can be achieved if the focus becomes more protection and streamlined compliance.

References

Collmann, J. (2007). The federal information security management act of 2002 title III-information security, electronic government act, public law (P. L.) 107-347. Retrieved March 8, 2011 from http://www. himss. org/content/files/CPRIToolkit/version6/v7/D68_FISMA. pdfCornell University Law School (n. d.). U. S. code. Retrieved March 10, 2011 from http://www. law. cornell. edu/uscode/usc_sec_44_00003541—-000-. htmlGovITWilki (2008). Federal information security management act. Retrieved March 10, 2011 from http://govitwiki.

com/wiki/Federal_Information_Security_Management_Act Hasson, J. (2008). FISMA – The basics. Retrieved March 7, 2011 from http://www. nextgov. com/the_basics/tb_20080502_8349. php IBM Corporation (2007). FISMA compliance a holistic approach to fisma and information security. Retrieved March 14, 2011 from http://docs. govinfosecurity. com/files/whitepapers/pdf/413_fisma_whitepaper. pdfMcDonald, S. (2010). (H. R. 3844) federal information Security management act OF 2002: statement submitted for the record. Retrieved March 13, 2011 from || http://www. gsa. gov/portal/content/100950National Institute of Health (2009). Federal information security management act and agency privacy management (FISMA). Retrieved March 13, 2011 from http://oma. od. nih. gov/ms/privacy/fisma. html Rasmussen, M. (2010). Federal information security management act (FISMA) overview. Retrieved March 14, from http://docs. govinfosecurity. com/files/whitepapers/pdf/362_Six_Critical_Elements_to_Achieve_Economies_in_FISMA_Compliance_Lumension_011410. pdf|| TechTarget (n. d.). Federal information security management act. Retrieved March 7, 2011