ISSN:0971-1260
Vol-22-Issue-4-October-December-2019

The Study of Appropriate Potential Information Security Policies for Defending from Dark Cloud and Ensuring IT Security Assurance

Dr. Sunil Khilari [1] Dr.Sachin Kadam [2]

Abstract: *An information system is not just computer; todays information systems are complex and having many components those peripherals together to make business solution. The literature clearly agrees that the major threat to an organization's information security is caused by careless and sick minded employees who intentionally or unintentionally misuse the organization's information assets. This paper enlightens information security (IS) policies and processes that organizations should follow and also develop effective information security policies. Dire need of practicing good and emerging IS policies and their efficient and effective management has no any alternate option and has unique key concern for all organization. It is of course better to focus on prevention than cure.. In this paper, researcher provides an overview on information security policies that can prove usefulness in finding and fixing security flaws. Since adequate policies cannot be provided by technology alone, it is necessary to rely on a combination of hardware, software, and procedural practicner. The main goals of this paper are to identify some key IS policies and their usage in everyday life of digital generation and digital economy.*

Keywords*: Information security (IS), security policies, Information security assurance, dark cloud.*

1. INTRODUCTION

Organizations are extremely dependent on Information Technology (IT) as it supports day-to-day transactions and many critical business functions. IT stores confidential information related to everything such as organizations' financial records, medical records, job performance reviews, trade secrets, new product developments and marketing strategies etc., which all must be protected to ensure organization survival and growth.



 Copyright ⓒ 2019Authors

ISSN:0971-1260
Vol-22-Issue-4-October-December-2019

Figure-1: CIA in IS

Due to the lack of the IS security policy development guidance, IS security policy developers often use commercially available sources or templates accessible from the internet in order to develop their policies.

Information Security Policy (ISP) : is a set of rules enacted by an organization to ensure that all users within the organization's domain abide by the prescriptions regarding the security of data stored digitally within the boundaries the organization which stretches its authority.

An ISP is governing the protection of information, which is one of the many assets an enterprise needs to protect.

2. Purpose Information Security Policy (ISP)

ISP's need to create and practice for a variety of reasons:

- To observe the access of the customers; providing effective mechanisms for responding to complaints and queries concerning real non-compliances with the policy is one way to achieve the security and business objective
- To ascertain a general approach to information security
- To detect and anticipate the compromise of information security such as exploitation of data, networks, computer systems and applications.
- To protect the reputation, sensitivity, privacy and business secrete of the organization and individuals with respect to its ethical and legal responsibilities.

Security policies are the foundation basics of a resonance and effective implementation of security. Organizations usually implement technical security solutions without initially creating this foundation of policies, standards, guidelines, controls and procedures. Thus, unintentionally creating unfocused and ineffective security controls. To avoid this, security policies are required.

Information security objectives: An organization that strive to compose a working ISP needs to have well-defined objectives concerning security and strategy on which management have reached an agreement. Any existing dissonances in this context may render the information security policy project dysfunctional. The most important thing that a security professional should remember is that his knowing the security management practices would allow him to incorporate them into the documents he is entrusted to draft, and that is a guarantee for completeness, quality and workability.

 Copyright ⓒ 2019Authors

ISSN:0971-1260
Vol-22-Issue-4-October-December-2019

Management views IT security seems to be one of the first steps when a person intends to enforce new rules in this department. Furthermore, a security professional should make sure that the ISP has an equal institutional gravity as other policies enacted within the corporation. In cases where an organization has sizeable structure, policies may differ and therefore be segregated in order to define the dealings in the intended subset of this organization.

Information security is deemed to safeguard three main objectives:

- Confidentiality – data and information assets must be confined to people authorized to access and not be disclosed to others;
- Integrity – keeping the data intact, complete and accurate, and IT systems operational;
- Availability – an objective indicating that information or system is at disposal of authorized users when needed.

3. THE INFORMATION SECURITY CHALLENGES

Information or Cyber security is major national, international and economic security issue of all concerns. Protecting assets and managing access to IT resources has more important. Dark cloud is expanding the attack surface and breaking traditional network boundaries. Need to check whether our current security architectures mitigate the threats and vulnerabilities.

The confidentiality, integrity and availability of information, in all its forms, are critical to the on-going functioning and good governance of LSE. Failure to adequately secure information increases the risk of financial and reputational losses from which it may be difficult for LSE to recover.

This information security policy outlines LSE's approach to information security management. It provides the guiding principles and responsibilities necessary to safeguard the security of the School's information systems. Supporting policies, codes of practice, procedures and guidelines provide further details.LSE is committed to a robust implementation of Information Security Management. It aims to ensure the appropriate conf

4. INFORMATION ASSURANCE (IA) VS. SOFTWARE SECURITY ASSURANCE (SSA)

When management choose to beat competition by giving their employees increased access to business critical resources, it also felt the need to conduct a security audit to get a closer look at the strength and weakness of the current infrastructure along with advice on strategies and

 Copyright ⓒ 2019Authors

ISSN:0971-1260
Vol-22-Issue-4-October-December-2019

polices required to stay competitive. In this scenario Information assurance and software security assurance plays vital role.

Table No.1: IA vs.SSA

Information assurance (IA)	**Software Security Assurance** (SSA)
The practice of assuring **information** and managing risks related to the use, processing, storage, and transmission of **information** or data and the systems and processes used for those purposes	The process of ensuring that **software** is designed to operate at a level of **security** that is consistent with the potential harm that could result from the loss, inaccuracy, alteration, unavailability, or misuse of the data and resources that it uses, controls, and protects

5. DARK CLOUD

"Dark Cloud" computing networks, known as botnets. Can run millions of infected computers, called bots which spread malware. Its take-up is still being held back by much fear, uncertainty and doubt among not just potential cloud users, but also some policymakers and regulators. It's been a few years since cloud computing hit the IT scene like rolling thunder, but many businesses still struggle with making the move to the cloud. A server that is not in-house is less secure. The cloud is very expensive. If someone else is managing the data, you don't need an in-house IT staff.

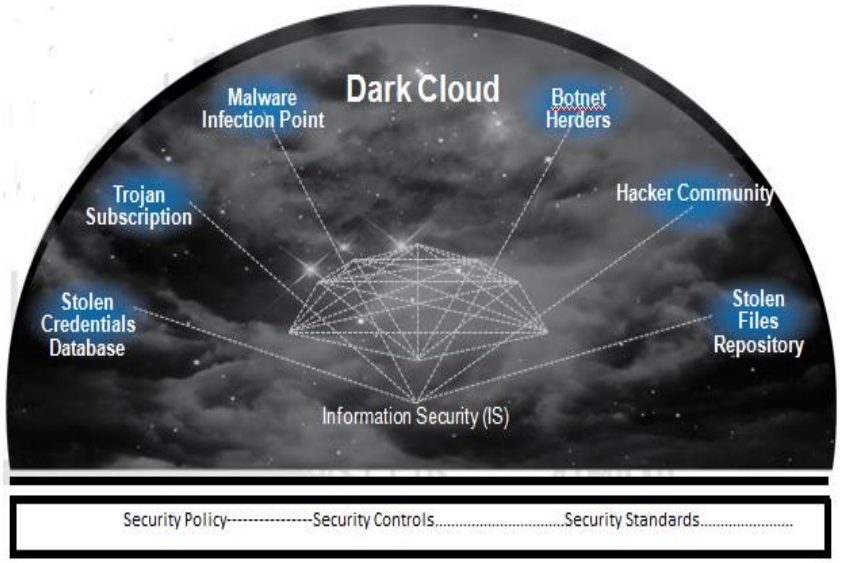


Figure-2: Dark Cloud in Information Security (IS)

Copyright ⓒ 2019Authors

ISSN:0971-1260
Vol-22-Issue-4-October-December-2019

Present technology offers no way to absolutely protect information or the computer operating system itself from *all* security threats posed by the human beings around it. As a consequence, procedural and administrative safeguards must be applied in resource sharing computer centers to supplement the protection available in the hardware and software. .problems of security is admittedly most acute at. Present, must be designed to protect each user from interference by another user or by the system itself, and must provide some sort of "privacy" protection

To users who wish to preserve the integrity of their data and their programs. Thus, designers and manufacturers of resource-sharing systems are concerned with the fundamental problem of protecting information.

In protecting classified information, there are differences of degree, and there are new surface problems, but the basic issues are generally equivalent. The solutions the manufacturer designs into the hardware and software must be augmented and refined to provide the additional level of protection demanded of machines functioning in a security environment.

6. INFORMATION SECURITY POLICIES DEVELOPMENTS AND IMPLEMENTATIONS

Many policies can be applied during software development to ferret out and fix problems. So let us begin by looking at the nature of development itself, to see what tasks are involved in specifying, designing, building, and testing software. The Nature of Software Development Software development is often considered a solitary effort; a programmer sits with a specification or design and grinds out line after line of code. But in fact, software development is a collaborative effort, involving people with different skill sets who combine their expertise to produce a working product. Development requires people who can

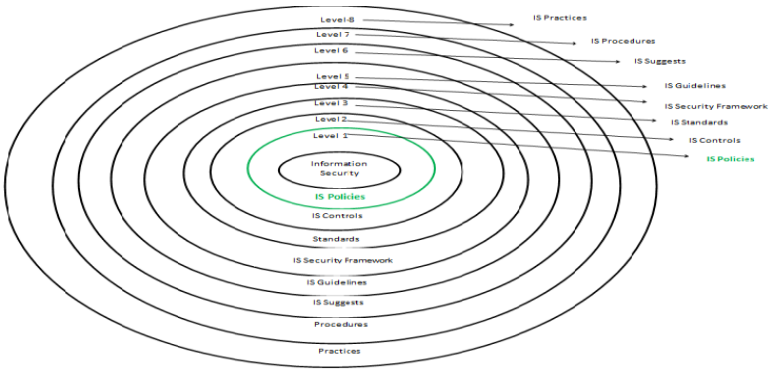


Figure-2: Levels of defense in IS

- specify the system, by capturing the requirements and building a model of how the system should work from the users' point of view

Copyright ⓒ 2019Authors

ISSN:0971-1260
Vol-22-Issue-4-October-December-2019

- design the system, by proposing a solution to the problem described by the requirements and building a model of the solution
- implement the system, by using the design as a blueprint for building a working solution
- Test the system, to ensure that it meets the requirements and implements the solution as called for in the design
- review the system at various stages, to make sure that the end products are consistent with the specification and design models
- document the system, so that users can be trained and supported
- manage the system, to estimate what resources will be needed for development and to track when the system will be done
- maintain the system, tracking problems found, changes needed, and changes made, and evaluating their effects on overall quality and functionality

One person could do all these things. But more often than not, a team of developer's works together to perform these tasks. Sometimes a team member does more than one activity; a tester can take part in a requirements review, for example, or an implementer can write documentation. Each team is different, and team dynamics play a large role in the team's success.

We can examine both product and process to see how each contributes to quality and in particular to security as an aspect of quality. Let us begin with the product, to get a sense of how we recognize high quality secure software.

These Standards impose compliance obligations upon Entities. However, discretion and good judgment are required as to what resources are applied, and in what configuration, in order to achieve those obligations and to implement the additional policies judged necessary by the Entity. Entities need to determine what organization structure best suits achievement of its own Information Security Programme Plan. Examples where decision making is required include:

• Whether the mandate of the Information Security Governance Committee should be addressed by a free-standing committee or incorporated into the functioning of an already existing committee. • Whether the role of Chief Information Security Officer (CISO) should be full or part time. • Whether the CISO role should be rendered at corporate-level or within an individual business unit (e.g. the IT department). • Whether the level of risk, programme goals and level of activity provide justification for additional security-related resources, beyond the CISO. • What weighting should be applied to Information Security roles i.e. technical vs. managerial. • What

Copyright ⓒ 2019Authors

ISSN:0971-1260
Vol-22-Issue-4-October-December-2019

minimum level of experience, competence and qualifications post-holders require in order to successfully achieve the goals of the Entity's Information Security Programme.

A one-size-fits-all approach is not practical, given the diversity of Abu Dhabi Government Entities, in terms of their remit, structure, risk profile and resources.In the above context, security domains described within these Standards should not be taken to be equivalent to specific organizational roles or units. For example, obligations applicable to Information Security Incident Management may be undertaken by a function that has responsibility for all types of incident across the Entity. Similarly, Asset Management obligations do not imply that separate and demarcated Asset Management provisions need to be created solely for the purpose of achieving alignment with the Asset Management expectations of these Standards.

7. TYPES OF SECURITY POLICIES

In fact, there is special concern about the risk of compromise of classified information and the vulnerability of an open system to potential penetrations because, as of today:

(a) It is virtually impossible to verify that a large software system is completely free of errors and anomalies.

(b) The state of system design of large software systems is such that frequent changes to the system can be expected.

(c) Certification of a system is not a fully developed technique nor are its details thoroughly worked out.

(d) System failure modes are not thoroughly understood, catalogued, or protected against.

(e) Large hardware complexes cannot be absolutely guaranteed error-free.

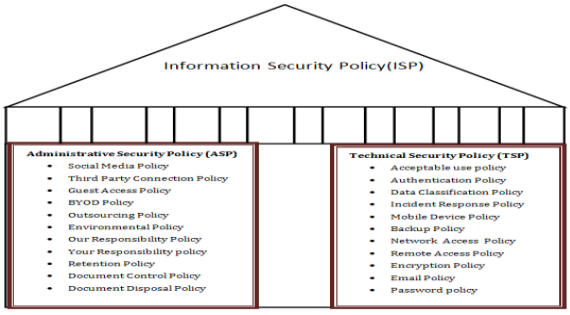


Figure-3: Types of IS policies

Security policy is an overall general statement produced by senior management, a selected policy board, or committee of an organization that dictates what role security plays within that organization. There are certain factors that security policies should follow, namely:

- Very generic, non-technical and easily understood

 Copyright ⓒ 2019Authors

ISSN:0971-1260
Vol-22-Issue-4-October-December-2019

- Provides "missions statement for security"
- Should represent business objectives
- Developed to integrate security into ALL business functions and processes
- Reviewed and modified as company changes
- Dated and version controlled
- Forward thinking

There are different types of security policies, namely:

- Regulatory
- Advisory
- Informative

The precise mix of policies and safeguards necessary in any given case will depend on the operational environment, sensitivity of information, <;lass of users, and types of service rendered, as noted above. We believe that these recommendations are both necessary and sufficient for a closed secure system. However, their sufficiency for an open system cannot be guaranteed in the abstract. Only by intelligent adaptation to a specific open environment utilizing experience from closed systems and by extremely objective and stringent testing and evaluation can their adequacy be established for a specific open system.

8. CONCLUSION

Organizations need to follow in developing and implementing an effective information policy. Organization must implement policies to reduce damage as well as develop incident response plans and business continuity plans. The IS policies should periodically be scrutinized and updated, and risk analysis perform. A high-grade ISP can make the difference between growing business and successful one. Improved efficiency, increased productivity, clarity of the objectives each entity has, understanding what IT and data should be secured and identifying the type and levels of security required and defining the applicable information security best practices are enough reasons. IS security effort is mainly reduced because security controls have to be modeled only once and afterwards they can be used for different policy analysis.

Information security awareness is an essential and a foundational element in assuring the nation's information assets are protected and always ready to meet mission objectives. The study on Information security awareness in business found several important issues that need to be addressed. Although the technical staff and employee staff are having the basic knowledge of security, still they are not aligned to the security practice of the organizations.

 Copyright ⓒ 2019Authors

ISSN:0971-1260
Vol-22-Issue-4-October-December-2019

If you want to lead a prosperous company in today's digital era, you certainly need to have a good information security policy at place.

9. REFERENCES

1. Bulgurcu, B., Cavusoglu, H. and Benbasat, I. (2010). "Information Security Policy Compliance: An empirical study of rationality-based beliefs and information security awareness". *MIS Quarterly*, 34(3), pp. 523-548
2. Baker, W. H., & Wallace, L. (2007). Is information security under control? Investigating quality in information security management. *IEEE Security & Privacy*, *5*(1), 36-44.
3. Bayuk, J. (2009). "How to Write an Information Security Policy". *Computerworld*.
4. Scott, A. (2013). *How to create a good information security policy*. Retrieved on 04/06/2014 fromhttp://www.computerweekly.com/feature/How-to-create-a-good-information-security-policy
5. Sophos Ltd. *SophosLabs Information Security Policy*.Retrieved on 04/06/2014 fromhttp://www.sophos.com/en-us/legal/sophoslabs-information-security-policy.aspx
6. Brykczynski, B. & Small, B. (2003). Securing your organization's information assets. *The Journal of Defense Software Engineering*, *16*(5), 12-16.
7. Diver, S. (2007). "Information Security Policy – A Development Guide for Large and Small Companies". *SANS Institute*. South Africa.
8. Mauritian Computer Emergency Team. (2011). "Guidelines on Information Security Policy". *Mauritius: National Computer Board*. CMSGu2011-04.
9. Bayuk J. (2009). *How to Write an Information Security Policy*. Retrieved on 04/06/2014 from http://www.csoonline.com/article/2124114/strategic-planning-erm/how-to-write-an-information-security-policy.html?page=2
10. A. Liu, "Change-impact analysis of firewall policies," in 12th European Symposium On Research In Computer Security, Dresden, Germany,September 24–26 2007, pp. 155–170.
11. Z. Li, X. Cui, and L. Chen, "Analysis And Classification of IPSec Security Policy Conflicts," in FCST06: Japan-China Joint Workshop on Frontier of Computer Science and Technology, Fukushimna, Japan,November 17–18 2006, pp. 83–88.
12. N. Ben Youssef, A. Bouhoula, and F. Jacquemard, "Automatic verification of conformance of firewall configurations to security policies," in 2009 IEEE Symposium on Computers and Communications, Sousse,Tunisia, July 5–8 2009, pp. 526–531.

 Copyright ⓒ 2019Authors