Journal of Engineering and Applied Sciences 13 (Special Issue 6): 5238-5242, 2018
ISSN: 1816-949X

A Perspective Study on Organizational Security Awareness and Measures

M. Nisha and S. Poongavanam
AMET Business School, AMET University, Chennai, India

Abstract: This study investigates the hole between hierarchical procedures and security outline. It begins with an introduction focusing on the requirement for enhanced security in the enterprise. Hierarchical procedures for example, work outline inventiveness, development, culture, learning and change are considered in authoritative plan. The way the association is planned and composed prompts the capacity to achieve its objectives. Many variables impact the conduct and execution of the association including the unique situation, reason individuals and structure as they interface with the center change and administration bolster procedures to set the association's execution level. This study focuses on organizational level to individual level. In the current world technology advancement, we planned to identify key security considerations and measures on the organization must be aware of organizational privacy.

Key words: Organizational privacy, culture, aware, inventiveness, technology advancement, organizational level, individual level, aware

INTRODUCTION

Most everything of substantial incentive in today's general public is put away in computerized frame some place. Without the information to protect our computerized resources, we are lost and our potential misfortune becomes bigger ordinary as we pour the substance of our lives into databases, PDAs, PCs and Web servers through switches, centers, PDAs, passages, copper, persuade and the air itself. The requirement for security has existed since, presenting the main PC. The worldview has moved as of late, however, from terminal server centralized computer frameworks to customer/server frameworks, to the broadly disseminated Internet.

In spite of the fact that security is imperative, it has not generally, been basic to an organization's prosperity. As innovation created and the cost of framework assets diminished, this issue turned out to be less imperative. Remote access to frameworks outside an organization's system was practically non-existent. Also, just the underground group had the learning and apparatuses expected to trade off a centralized computer framework. Late occasions have driven data security to wind up noticeably a critical concentration in the way an association leads its business. Security today ought to be joined with the texture of a business. In doing as such data security programs need to move from strategic usage of innovation to key accomplices in business. In spite of the fact that organizations were focused on building up a far reaching data security program, they might not have incorporated them into the system of their organizations.

This study is researched by following studies by Hong *et al.* (2003) integrated security policy assumptions, control, theory auditing theory, management system related theory and contingency theory for building a inclusive theory of security management in accordance with information. The research suggested for an integrated system theory for information security management approach and predicting solutions in the business. Ernest and Young (2002) revealed the significant impacts of organizational factors that also included the IT competence of business managers, uncertain environment industry type and that of organizational size on the effectiveness to implementing Information Security Management (ISM). Gordon *et al.* (2006) addressed the major issues considered in previous surveys where leaded to analyze important computer trends on security. The longer-trends considered in the survey included: unauthorized access to the computer systems, several incidents from outside and inside to the organization. Attack types detected and also, misused far responsiveness to computer intrusions.

Garg *et al.* (2003) developed an approach and thorough evaluation in IT security. The research depicted several new perspectives concerned with the

Corresponding Author: M. Nisha, AMET Business School, AMET University, Chennai, India

market view and reaction towards the breaches in IT security. The research extended to security vendors and a fuller exploration of market reactions before and after the denial of service attacks.

By Hu *et al* described a inclusive form of information security policy violation by employees in organizational settings based on multiple criminological theories. Davis (2005) explained about how to seek the enemies for a business. The research demonstrated PREPARE Model of Technology Crisis Management (TCM) along with the technology of the Johari Window psychology model that offer a business leaders methods which increases awareness of potential threats to their business. Computerworld, Inc (2007) identified the antecedents of employee compliance in accordance with ISP meant Information Security Policy for an organization. The research also, investigated the impact of Information Security Awareness (ISA) on the outcome belief and that of employee's attitude toward compliance with the security policy. Cassidy (1998) developed theoretically and tested empirically an Information Security (IS) Model for effectiveness that incorporates organization causes. The study assessed the sufficiency and efficacy in different organizations security measures and suggested several improving techniques for improving IS security effectiveness.

Brint Institute (2007) demonstrated an architecture sustaining knowledge of IT security for enhancing security information systems. The architecture utilizes customized set of processes for security aspect, provided security policies and security solutions for protecting organization's business. The architecture captured the security related knowledge for the purpose of sharing it and transfers it across the organization. Guenther (2004) founded an approach that revealed deeply well-established thoughts for preventive frame of mind, ensuring availability of technology and services and that of comparative ignorance of exposure to business security issues and risks. Belsis *et al* (2005) established a field search involved around five organizations included public and private and around five security experts and consultants in range. The research demonstrated the model illustrated the IS knowledge in an organization. Most organizations today have no less than a simple security program set up and many projects are creating and developing in development. As these projects have developed, so, wants to move past the view that security is only a specialized issue (Philip and Mani, 2017). By Poongavanam (2017) a centralized server framework, the firm shielded their frameworks from asset mishandle, for example, approved clients hoarding assets or unapproved clients getting entrance and utilizing save assets. Such mishandle was harming in light of the fact that framework assets were expensive in the beginning of centralized computers.

MATERIALS AND METHODS

Information in Technology (IT) framework is at hazard from different sources client mistakes and noxious and non-malignant assaults. Mis-chances can happen and aggressors can access the framework and can upset administrations, make frameworks futile or change, erase or take data. A few organizations have taken an edified perspective of security. They trust that, to be effective, they should demonstrate their clients that security and ensuring data resources are a center business work. Security by configuration implies that it is not reconsideration in the outline procedure, rather, it is one of the necessities that fashioners utilize when beginning a venture. Secure in organization implies that items will be delivered and prepared to use in a way that won't trade off the security of the client or different items.

Confidentiality: Secrecy is averting unapproved utilize or exposure of data. The framework contains data that calls for security from unapproved revelation. Illustrations incorporate planned dispersal data (e.g., break monetary articulations individual data and restrictive business data). Security is a firmly related subject that has recently been getting greater perceiviability.

Integrity: Trustworthiness is guaranteeing that data is precise and finish and that it has not been changed by unapproved clients or procedures. The framework contains data that must be shielded from unapproved, unforeseen or inadvertent change. Cases incorporate review reports, monetary markers or money related exchanges frameworks.

Availability: Accessibility is guaranteeing that clients have convenient and dependable access to their data resources. The framework contains data or gives benefits that must be accessible on an opportune premise to meet mission prerequisites or to keep away from generous misfortunes. Cases incorporate online openness of business records, frameworks basic to security, life support and tropical storm gauging.

These three components are the fundamentals around which all security projects are created. The three

ideas are connected together in data security. The possibility that data is a benefit that calls for insurance, much the same as other resource of the business is fundamental to understanding these ideas.

In characterizing reason, we consider how the association translates the earth to create explanations of mission, vision, objectives, procedures, targets and strategies. Despite the fact that the association's central goal may change gradually, vital signs to representatives are picked up from formal correspondences from administration about objectives and needs. Most business associations have vital arrangements that consolidate IT. Customarily, however, the IT part does exclude a security arrange. Rather, security is thought to be in the IT foundation. Deliberately, official administration should be sure that all outside and inside dangers have been tended to through a data security plan and arrangement. The entryway to the outside world is regularly a progression of resistances for example an external firewall, a middle of the road zone in the middle of to channel internet movement and another firewall to control the contacts between the organization and the outside world. The subsequent stage is to check that the operations in the association have safety efforts set up. Choices for gathering clients and giving access rights and the capacity to change basic information are regularly appointed to a security expert. This expert doubtlessly does not see the workings of the association in a full scale sense and he or she no doubt is not vested with the specialist or learning to adjust the corporate structure to the security structure. This study focuses on organizational level to individual level. In the current world technology advancement, we planned to identify key security considerations and measures on the organization must be aware of.

RESULTS AND DISCUSSION

An appropriately executed security framework can turn into an upper hand, giving assurance to corporate resources that set the organization with the exception of its rivals. On the off chance that an organization's fundamental rival is hoping to dispatch e-Business activities, the organization with the more grounded security foundation will be more fruitful. To begin with, the organization with the weaker security foundation may be more hesitant to dispatch e-Business ventures since, it is worried with security and does not know how to ensure itself satisfactorily. Second and all the more usually, the weaker organization will disregard the security part of online business and afterward ask why it endured an effective assault against its frameworks. This negligence could prompt the bargain of basic touchy information perhaps client's charge cards or business ledger numbers and the resulting loss of clients. The organizations with the more grounded security condition can all the more securely dispatch an online business activity, realizing that its corporate security foundation is sufficiently solid to ensure it. In the event that its frameworks do happen to be traded off, the business reaction arranges set up ought to bring down the harm. This study focuses on organizational level to individual level. In the current world technology advancement, we planned to identify key security considerations and measures on the organization must be aware of. Thedifferent security types are:

Data protection and recovery: Practices to protect data include continues network monitoring, guidelines in place, best practices training and testing and strict network policies. With the support of organizational effort for minimizing the risk on security issues, the organization need to align its way to follow mandated regulations for protecting its resources. For avoiding the security threats an organization should not only implement one type of measure, rather, recommended to provide several layers of protection for effective measure.

Cryptography: Cryptography or also, known as encryption techniques is one of more basic methods for protecting the information on the computer from unauthorized viewers. If a computer systems are illegally accessed a computer system leaded to stolen of data. There exists many kinds of threats like Trojan, Spyware, virus etc. to overcome this, cryptography came into existence providing secure communication of data.

Firewalls: While setting up the information technology security in an organization, firewalls are an efficient to secure the information and avoid many threats. Without setting up a firewall, the workplace will be highly susceptible to hackers and viruses while business moves into online. In fact setting up a firewall is a first step in making sure an organization's network system is secure and safer in establishing.

Network monitoring: Network monitoring is the method of monitoring a computer network for time-consuming

Table 1: The analysis of different security types

Security types	Feature	Advantages	Disadvantages	Application compatibility
Data protection and disaster recovery	Cloud disaster recovery afford working in a degraded mode	Less downtime Quick recovery times and data backup Cost containment Better inventory and network management	Only backup is possible on cloud File Collaboration tools needed to acquire	Yes
Cryptography	Elliptic curve cryptography quantum computation	Confidentiality Authentication Data integrity Non-repudiation	It difficult to access even for a legitimate user Selective access control Threats that emerge from the poor design of systems	Yes
Firewalls	Provide application function control Scan for viruses and malware in applications Deal with unknown traffic Identify and control applications sharing the same connection	Cheaper Ideal for personal or home use Easy to configure or reconfigure Cost savings	Takes up system resources It is unable to remove or un-install a firewall completely Not suitable where response times are critical Security cannot be achieved 100 %	Yes
Network monitoring	Streamline hands-on administration Increase system availability Optimize storage and similar resources	Speed Flexibility	Connectivity becomes tedious process System performance is reduced	

components insecure components, failing components and the breaches, that also, notifies the administrative network administrators by installing alarm systems in case of occurrences of threat.

Organizational security: In the process of protecting the organization from various kinds of security threats in foremost the organization need to aware employees to understand and follow security procedures, learning about information security will helps in preventing in prior and also solving the issues by understanding different types of cyber threats and attacks.

The different security types have their own features, advantages disadvantages and the application compatibility which is mentioned in Table 1. Among the other security types, the analyzed security types provide application compatibility which will be effective for the organizational security.

CONCLUSION

As security is a paramount concern for organizations as most organizational activities, business processes and other resources are valuable and are highly prone to threat among competitors intruders etc., issues on security have growing exponentially in the past years due to the fact that information is been converted electronically lead to easily accessible by unauthorized users. This leads the organization hesitant to expand its business online especially, to the small scale organizations. But this has to be overcome by many measures on organization security that leads to take the organization in wider spread across the world without the threat of security issues. For maintaining a high level security, it is necessary for an organization to implement security measures. The security measures like firewalls, network monitoring, encryption, data protection, disaster recovery and educating employees were analyzed and proved that these measures achieve highest level of organizational security.

REFERENCES

Belsis, P., S. Kokolakis and E. Kiountouzis, 2005. Information systems security from a knowledge management perspective. Inform. Manage. Comput. Secur., 13: 189-202.

Brint Institute, 2007. Business technology management and knowledge management research network. Brint Institute, Washington, D.C., USA.

Cassidy, A., 1998. A Practical Guide to Information Systems Planning. St. Lucie Press, Boca Raton, Florida, ISBN:1-57444-133-7, Pages: 283.

Computerworld, Inc., 2007. IT world. Computerworld, Inc., Washington, DC., USA.

Davis, B.J., 2005. Prepare: Seeking systemic solutions for technological crisis management. Knowl. Process Manage., 12: 123-131.

Ernst and Young, 2002. Global information security survey. Ernst&Young, London, UK.

Garg, A., J. Curtis and H. Halper, 2003. Quantifying the financial impact of IT security breaches. Inf. Manage. Comput. Secur., 11: 74-83.

Gordon, L.A., M.P. Loeb, W. Lucyshyn and R. Richardson, 2006. CSI-FBI computer crime and security survey. Comput. Secur. J., 22: 1-1.

Guenther, M., 2004. Security-privacy compliance: Culture change. EDPACS., 31: 19-24.

Hong, K.S., Y.P. Chi, L.R. Chao and J.H. Tang, 2003. An integrated system theory of information security management. Inf. Manage. Comput. Secur., 11: 243-248.

Philip, P. and A. Mani, 2017. Connect among employee engagement and three key of organisational commitment level an empirical exploration AMID techs. Intl. J. Mech. Eng. Technol., 8: 296-303.

Poongavanam, S., 2017. The influence of internal locus of control on personal and job orinted factors. Intl. J. Econ. Res., 14: 273-279.