Separate organization computing environment into zones information technology ess...

Technology, Information Technology

Abstract: Information security refers to how the information that user supply will be protected, give user information to someone else? Will sell it? Will keep it private and not give it to anyone? Will give others only part of user information. This paper has specifically focused on the information security in organization such as current issues, challengers, and recommendations to avoid problems in security of information. Now information security in organization also less concentrate because the people don't think about effect in future if the staff not cares about information in organization. So this paper reviews about important of information security in organization.

Keywords: Information security, information in organization, issues information security

Introduction

Nowadays, information security is a big issue among people, especially information security in computer technology. Information security that's means is the practice of maintain information from unauthorized access, use, disclosure, disruption, edit, perusal, inspection, recording or destruction. It is the words can be used another way of the form the data may take which is electronic or physical. Other than that, another terms relates with information security is information technology security. Information technology security actually information security when use to technology basically computer systems. The problems in information security now are lack of awareness, in corporate level and in end user level. Organizations must ensure understand the threat as it really is today, not as they think it is. Organizations must to ensure their users are educated to use the internet and internet resources from a position of awareness and caution rather than blind trust in a technological solution. User must be aware of how invisibly infections can occur and where to go if they are concerned they may be a victim. So people need to be made aware of the real monetary value of their own and other people's personal information and begin to treat it with the care it deserves, rather than offering it to any curious onlooker through social and professional networking, blogging, telephone calls, bogus surveys and more. The second problems in information security is complacency, when it comes to losing data, either as a result of malware of " peopleware" many companies suffer from being complacent. This ties in very strongly to my first point of education. It is important and in many cases legally or regulatorally necessary to protect the data for which company are responsible. This data can fall into more aspects Personally Identifiable Information (PII), Intellectual Property, corporate, state or nationally sensitive information, financial results, login credentials, patient or customer information, the list is almost endless. The organizations have their own corpus of data and the relevant obligation to protect that corpus from both inadvertent and malicious exposure and or misuse. Now many companies are being too complacent in this area and are only prompted into action when a breach or a near-breach has occurred. Organizations must to be able to manage patch levels of all machines within their estate at a moment's notice and also must be deploying host-based Intrusion Prevention technology in areas where patching is impractical or impossible. Other than that, there is a responsibility to both staff and to customers to make sure that they have full visibility over how data is managed under their custodianship and this includes all the ad-hoc transfers that take place every day over services like email, HTTP, FTP, Instant Messaging, USB devices.

Methodology

In completing this term paper, I used three different methods to understanding the topic which is literature review, gain knowledge and observation. For the first methods is literature review. I used internet as a tool to find the article relate to my topic entitled information security and the three article I refer is Information security and business continuity management in interorganizational IT relationships, second article Information system security issues and decisions for small business and the third article is Knowledge management systems: Issues, challenges and benefits Information management & computer security. I review the all information from the article and combine also create the new information understanding but still relate with the topic. The all information in internet is not accurate but I should evaluate before I state in term paper. The second methods I use are gain knowledge. To complete the term paper I ask my friends about information security and they give opinion about this topic. Other than that, we also make the discussion to gain knowledge about this topic and after that we review about the discussion. The last method is observation based on the situation. From my observation I think much organization less knowledge about information security because they not involve in programmed that the agencies provide, so from this situation the security in organization is opened and the hackers will be easy to hack.

Definitions and concepts of information security

Information security (InfoSec) is the practice of defending information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. It is a general term that can be used another way of the form the data may take electronic, physical, etc. Another term of information security is it security, it is referred to as computer security, according to www. wikipedia. org, information technology security is information security when use to technology.. A computer is any device with a processor and some memory. IT security specialists are almost always found in any main enterprise or establishment due to the nature and value of the data within larger businesses. They are responsible for save all of the technology within the company secure from malicious cyber attacks that often attempt to breach into critical private information or get control of the internal systems. The others term is security management, according to Barlas, Queen, Randowiz, Shillam & Williams 2007 is defined as a " systematic approach to encompassing people, process and information technology systems that safeguards critical systems and information protecting them from internal and external threats. The first concept of information security is confidential. Confidentiality means that information that must stay secret stays secret and only those persons authorized to access it may receive access and in our information age, access to information is more important than ever. Unauthorized access to confidential information may have devastating consequences, not only in national security applications, but also in commerce and industry. The second concept is Integrity is concerned with the trustworthiness, origin, completeness, and correctness of information as well as the prevention of improper or unauthorized modification of information. Integrity in the information security context refers not only to integrity of information itself but also to the origin integrity. Integrity protection mechanisms may be grouped into two broad types, preventive mechanisms, such as access controls that prevent unauthorized modification of information, and detective mechanisms, which are intended to detect unauthorized modifications when preventive mechanisms have failed. Controls that protect integrity include principles of least privilege, separation, and rotation of duties. Next concept is Identification is the first step in the identify-authenticate-authorize sequence that is performed every day countless times by humans and computers alike when access to information or information processing resources are required. While particulars of identification systems differ depending on who or what is being identified, some intrinsic properties of identification apply regardless of these particulars—just three of these properties are the scope, locality, and uniqueness of IDs. After that Authentication, that means which happens just after identification and before authorization, verifies the authenticity of the identity declared at the identification stage. In other words, it is at the authentication stage that you prove that you are indeed the person or the system you claim to be.

Ethics Conceptual Theory

IdentifyPolicy and StandardMonitorAssessProtectDiagram 1 Security life cycle

Challenges in Encouraging information security Among Information / Information Technology Personnel

There are several challengers in information security identified is combining corporate and personal life, IT does not own and control all devices, internal vs. external vague, challengers is secret attack and government legislation and industry regulations. 5. 1 Combining corporate and personal lifeIt is more difficult to distinguish between work life and personal life as the days have less of a different start and end. For example, employees use company email for some personal communications, and some workers may remove blackberry or mobile phones they use for limited personal use. Many people may not have a computer at home and use their company manufactures laptops for everything including conducting personal software, such as their tax software. On the flip side, some employees may bring a personal laptop to the office and try to plug it in. Inconsistent enforcement policies, many organizations are either not enforced their policies in the past, or have done so inconsistent depending on the position of the employee. This causes a lot of issues when trying to disable security functions offenders5. 2 IT does not own and control all devicesIT does not own and control all devices referred to this issue on a personal mobile device, but what if the organization does not provide the PDA to the sales team, so they buy their own and start a list of customers keep on top of it and try to connect to your wireless network at the office. 5. 3 Internal versus external vagueAdvantage or perimeter network is not so clear anymore. In the past we create a strong perimeter controls to control access into and out of the network, but now that the perimeter has been pushed out to their friends with extranets, to a third party hosting service, and the employees home with a VPN solution that can use of personal computers. 5. 4 Secret attackSecret attack is no longer clear. It used to be common for a viral infection to be big and messy cause a lot of damage and immediately becomes apparent when you have been infected. Now however, are silent attackers and quietly. They do not want to delete user data or take down user system, they want to slowly steal data or use user computer's power to attack other victims. They are doing their best to be undetectable by the rootkit and backdoor Trojans. 5. 5 Government legislation and industry regulations. New information security incidents and increased reliance upon the internet have encouraged governments around the world to create additional legislation to regulate the technology ecosystem. This legislation spans broad areas, like consumer privacy, to specific regulations for industries, like health care and financial services because the internet is easily accessible at more places, it is important to understand and operate in compliance with these regulations

Recommendations to Address the Challenges in Encouraging Ethical Behaviors Among Information / Information Technology Personnel

In response to these challenges, the main recommendations are proposed as follows which is administrative, logical and physical control and the others recommendation is make sure the CEO know the information security management and Separate organization computing environment into zones. 6. 1 Administrative control. Administrative controls also called procedural controls consist of approved written policies, procedures, standards and guidelines. Administrative control inform people on how the email in organization and how day to day operations are to be conducted. Laws and regulations created by government bodies are also a type of administrative control because they inform the rules. Some industry sectors have policies, procedures, standards and guidelines that must be followed. Other examples of administrative controls include the corporate security policy, password policy, hiring policies, and disciplinary policies. 6. 2 Logical control. Logical controls also called technical controls, use software and data to managed and control access to information and computing systems. The organization control through passwords, network and host based firewalls network intrusion detection systems, access control lists, and data encryption are logical controls. The benefits of logical control that is frequently overlooked is the principle of least privilege. The principle of least privilege requires that an individual, program or system process is not granted any more access privileges than are necessary to perform the task. This happens when the staff transfer to another department or change to higher level. 6. 3 Physical control. Physical controls managed and control the environment of the work place and computing facilities. They also monitor and control access to and from such facilities. For example doors, locks, heating and air conditioning, smoke and fire alarms, fire suppression systems, cameras, barricades, fencing, security guards, cable locks and so on. Separating the network and workplace into functional areas are also physical controls. An important physical control that is frequently overlooked is the separation of duties. Separation of duties ensures that an individual can not complete a critical task by himself. For example: an employee who submits a request for reimbursement should not also be able to authorize payment or print the check. An applications programmer should not also be the server administrator or the database administrator. These roles and responsibilities must be separated from one another6. 4 Make sure the CEO know the information security management. The CEO must detail know about information security management to avoid if something wrong happen in organization. If the CEO don’t know the organization will be destroy and cannot develop. The objective of the Information Security Management is to ensure that IT security is consistent with business security, ensuring that information security is effectively managed in all service and Service Management activities and that information resources have effective stewardship and are properly used. This includes the identification and management of information security risks6. 5 Separate organization computing environment into " zones." Security zones offer easy and flexible method for managing a secure environment. Organization can use security zones to enforce organization's Internet security policies, based on the origin of the Web content. Security zones enable organization to group sets of sites together and assign a security level to each zone. Grouping Sets of Sites Together that means Zone security is a system that enables organization or user to divide online content into categories, or zones. Organization can assign specific Web sites to each zone, depending on how much you trust the content of each site

Conclusion

As a conclusion information security actually is very important in organization because to protect data from user or customer. So if information safe in organization it is one of the investments from customer, they confident with organization because the all data will be protected from that organization. So all of the organization must be find the new alternative to protect information for develop their business. Other than that the staff in organization also must follow the guidelines provide from organization and also involved in security programmed. After that the government also must promote to people about important of information security and also give the fund to implement the all programmed. So if the country implement that guide truly, the information will be safe.