Securing and protecting information

Technology, Information Technology

Security and Protecting Information Securing and protecting information Development of information securitystrategies protecting complex data and information across a wide network while also improving system performance as well as ensuring easy data retrieval when necessary is one of the most challenging tasks in network design (Dhillon, 2007). This is even made worse by the porous and complex nature of modern transactions and the increasing demand for safe and secure information storage and retrieval mechanisms. The process of securing and protecting information refers to defending data and information from unauthorized access, disclosure, modification, inspection, use or destruction (Layton, 2007). Information security includes protection of all forms of information and data including both physical and electronic forms. Information security encompasses four main areas that aim at safeguarding the whole integrity of the information collected and stored for future retrieval. These are availability of the data and information on demand, confidentiality, accountability on the part of individuals charged with the responsibility of managing the information, and data integrity (Dhillon, 2007). A security authentication process refers to the process of determining he individuals authorized to access, retrieve, alter and use information at specified times and in a specified manner. The authentication process involves putting in place measures to determine which individuals are authorized to access the information stored. Creating a security authentication process for any piece of information comprises of various steps. The first step involves identifying the information that needs to be protected. This entails an organization examining its records to find out which set of information is vulnerable and therefore seek to protect it (Allen, 2001). This may be employee details, market research, and product information among others. The next step is conducting an analysis of security risks associated with the information identified as being vulnerable. The organization needs to determine what types of risks are likely to interfere with the information. This may include hackers, physical force, loss of data through accidents, leaking of information to unauthorized parties among others. The next step is developing a security plan in line with the risks associated with the information identified. The security plan includes timelines for implementing the security measures and details of what needs to be done. The process then moves to the next step of developing a security policy detailing the specific measures to be taken to safeguard the information (Dhillon, 2007). After developing the policy, the next step is to develop the procedures to be taken in order to implement the security policies enacted. The next step is to seek support from relevant people regarding the measures taken. This involves achieving buy in from both technical staff and the managers of the organization. The users of the systems developed to protect the information will then be taken through the next step which is training. The last step in the process is to implement the policies and maintain and protect the information. There are various methods that can be used to ensure authentication and authorization process is enabled and that the information is protected as required. Authentication involves determining if a user is indeed who he claims to be in order to grant him the authority to access the stored information. There are two main components of an authentication process. First the authentication process can determine which type of users ought to access the information and the type of information to be accessed. The other component is determining the time of access, such that the information can only be accessed at specified times by the authorized individuals. The two components can be implemented simultaneously or each as a single authentication element (McNab, 2004). An authentication process determines three main things before granting authority to an individual to access stored information. These include considering what issues the user knows, such as simple usernames and passwords; what the users has, such as smart cards; and the physical characteristics of the user such as finger prints. Consequently, authentication measures include mechanisms such as the use of usernames and passwords, biometric technology, single sign on systems (SSO), public key infrastructure and digital certificates (Layton, 2007). These authentication considerations will greatly affect the design and development process for new information systems in the future in various ways. First the need to protect information will be a very important factor in developing new system in order to maintain the confidentiality and integrity of information stored in the new systems. The new systems will also need to be highly structured such that the authentication process is reliable and effective in protecting data stored in it. There are other preventive measures for securing data and information such as backups and remote storage techniques. These methods are gaining popularity among system users and developers but also have their own share of disadvantages that need to be taken in to consideration such as the amount of resources needed for backup and redundant storage (McNab, 2004). These methods can also be more effective if they are used together with the authentication techniques identified so as to prevent unauthorized access. References Allen, J. H. (2001). The CERT Guide to System and Network Security Practices. Boston, MA: Addison-Wesley. Dhillon, G. (2007). Principles of Information Systems Security: text and cases. NY: John Wiley & Sons. Layton, T. P. (2007). Information Security: Design, Implementation, Measurement, and Compliance. Boca Raton, FL: Auerbach publications. McNab, C. (2004). Network Security Assessment. Sebastopol, CA: O'Reilly.