The thrust of the computer security plan

Engineering, Computer Security

The thrust of the Computer Security Plan part of the Business Plan is to ensure that the information systems to be deployed by the company will be in line with of the strategic mission and vision of the company. In order to insure that the informationtechnologyinfrastructure and resources will meet the requisite requirements of every strategic, tactical and operational plan, the company decided to start on the right footing by adapting the standards contained in the ISO/IEC 17799: 2005 or specifically known as the Information Technology - Security Techniques - Code of Practice for Information Security Management. By purchasing the ISO 17799 Toolkit, the company can follow the roadmap for a more secure information systemsenvironment, implement the policies contained in the toolkit, and eventually obtain ISO 17799 certification to add more value to the consulting business.

Specifically, the company will initially address the following areas that require immediate attention:

1. User authentication methods and policies - This will be based on Section 11. 1. 1 of ISO 17799 wherein, " An access control policy should be established, documented, and reviewed based on business and security requirements for access. Access control rules and rights for each user or group of users should be clearly stated in an access control policy. Access controls are both logical and physical and these should be considered together. Users and service providers should be given a clear statement of the business requirements to be met by access controls."

2. Desktop policies - This will be based on Sections 11. 3. 2 Unattended user equipment and 11. 3. 3 Clear desk and clear screen policy wherein, " Users should ensure that unattended equipment has appropriate protection. All users should be made aware of the security requirements and procedures for protecting unattended equipment, as well as their responsibilities for implementing such protection. Users should be advised to terminate active sessions when finished, unless they can be secured by an appropriate locking mechanism, e. g. a password protected screen saver; log-off mainframe computers, servers, and office PCs when the session is finished; secure PCs or terminals from unauthorized use by a key lock or an equivalent control. A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities should be adopted."

3. Remote user authentication methods and policies - This will be based on Section 11. 4. 2 User authentication for external users of ISO 17799 wherein, " Appropriate authentication methods should be used to control access by remote users. Authentication of remote users can be achieved using, for example, a cryptographic based technique, hardware tokens, or a challenge/response protocol. Possible implementations of such techniques can be found in various virtual private network (VPN) solutions. Dedicated private lines can also be used to provide assurance of the source of connections. Dial-back procedures and controls, e. g. using dial-back modems, can provide protection against unauthorized and unwanted connections to an organization's information processing facilities. This type of control authenticates users trying to establish a connection to an organization's network from remote locations."

4. Password policy - This will be based on Section 11. 3. 1 Password use of ISO 17799 wherein, " Users should be required to follow good security practices in the selection and use of passwords. All users should be advised to keep passwords confidential; avoid keeping a paper or software record of passwords, unless this can be stored securely and the method of storing has been approved; change passwords whenever there is any indication of possible system or password compromise; select quality passwords with sufficient minimum length which are easy to remember; not based on anything somebody else could easily guess or obtain using person related information; not vulnerable to dictionary attacks; free of consecutive identical, all-numeric or all-alphabetic characters; change passwords at regular intervals or based on the number of accesses, and avoid re-using or cycling old passwords; change temporary passwords at the first log-on; not include passwords in any automated log-on process, not use the same password for business and non-business purposes."

5. Communicationprocess for email, secure file exchange via email - This will be based on Section 10. 1. 1 Documented operating procedures of ISO 17799 wherein, " Operating procedures should be documented, maintained, and made available to all users who need them. Documented procedures should be prepared for system activities associated with information processing and communication facilities, such as computer start-up and close-down procedures, backup, equipment maintenance, media handling, computer room and mail handling management, and safety. Operating procedures, and the documented procedures for system activities, should be treated as formal documents and changes authorized by management.

Where technically feasible, information systems should be managed consistently, using the same procedures, tools, and utilities."

To further manage the information technology infrastructure and resources, the plan calls for the adoption of the " best-of-breed" approach by way of making certain that the building blocks of information security (Shaurette 2002) are fully exploited. These building blocks include the optimum use of security policies, authentication, access control, anti-virus/content filtering systems, virtual private networking (VPN)/encryption methodologies, vulnerability services consulting, intrusion protection system, and public key infrastructure (PKI)/certification authorities (CA)/digital signatures systems. This is considered to be the first step towards finding a technique for modeling and evaluating the security of a system (Stjerneby 2002).