System security criteria

Law, Security

Trusted Computer System Evaluation Criteria (TCSEC) is applied in classifying and evaluating the computer security in any given system especially where sensitive information is involved. For that reason any organization such as Medical Credential Company has to initially consider a few factors as well as meet security criteria as provided by TCSEC. There exists four divisions (D, C, B, and A) and C, B, and A are further divided into classes but in the context of this study, only classes C-2 (Controlled Access Protection) and B-3 (Security Domains) will be considered.

By choosing Class C-2 means that the company opts for Discretionary Security Protection which is under Division C. class C-2 offers defense of the sensitive information/data ‘ against and detection of user abuse of authority and direct probing’. Besides, class C-2 also protects the system form activities of non-users and users who may not be using malicious programs. Class C-2 employs security controls for all objects in the system which may be personal files and/or specific devices.

Subsequently, an individual is supposed to identify and authenticate him/her –self before login into the system and after using a track record of what he/she has done is kept. Therefore Class C-2 puts emphasis on audit trail for evaluation purposes. For that reason, it calls for a selective method to record all events which have occurred and tools to examine the audit record (DoD, 1985). On the other hand, Class B-3 which falls under Mandatory Security Protection, Division B, puts emphasis on security domains in the system.

Systems that conform to Class B-3 criteria enforce what Class C-2 criteria entails, discretionary security policies, and its policy. Therefore, Class B-3 is has more has security features compared to class C-2. Reason being

substantial confidence is created that the computer system is protected against misuse techniques for instance human error, direct probing, and abuse of authority by users.

In particular Class B-3 protects the system from intentional subversions of the computer security methods hence it is widely employed in addressing defense mechanisms against malicious programs. Besides, a computer system that meets security requirements for Class B3 entails security kernel which implements a reference monitor principle which lacks in Class C-2. Both of these classes entail security requirements -classified under policy, accountability, and assurance- aimed at regulating access to information.

Security policy, marking, identification, and accountability specify what control measures that needs to be put in place to regulate access to information. Besides, assurance and continuous protection provides guidelines on how a person can obtain credible assurance that overall security is achieved in a trusted system but security requirements in the two classes differ (DoD, 1985; Nibaldi, 1979). Figure 1.

Table of security requirements for classes C2 and B3. Legend: " x" -no requirement; "-" class has same requirements as the next lower class; " R"-class has extra requirement over the lower classes. NB: Adopted from DoD 5200. 28-STD The security requirements outlined in the above table are functionally-oriented and it is in order for the security manager of the company to consider employing security controls first.

Considering the security criteria employed by Class B3, as a security manager in the company, it would be better to seek certification for Class

B3. References DoD. (1985, December). DoD standard: Trusted Computer System Evaluation Criteria, DoD 5200. 28-STD. Retrieved August 22, 2010 from http://www. dynamoo. com/orange/fulltext. htm Nibaldi, G. H. (1979, November). Specification of A Trusted Computing Base, M79-228, AD-A108-831 (TCB), MITRE Corp. , Bedford, Mass.