|  |  |
| --- | --- |
|  | CIS-1290 Principles of Information Security |

Assignment 2

|  |  |
| --- | --- |
| To: | Mike MacDonald |
| From: | Christopher Sigouin |
| Date: | January 16, 2015 |
| Subject: | Rand Report Key Point Summary |
|  |  |

Prior to the Rand Report R-609 the military needed to protect the integrity of their data. In order to reach this objective a basis of physical security with simple document classifications was utilized. It effectively prevented theft, sabotage and espionage during that time. As time went on they required a method to better communicate information between systems. ARPANET was developed for this and created the first networked communication system. The system grew and became more popular including the ability to misuse it. Robert M. “Bob” Metcalfe identified many areas that were unexamined after his development of the Ethernet technology. The following areas are:

* + - Remote sites had no protection from an unauthorized remote user
    - Password issues with format and structure
    - Dial up connections had a lack of safety procedures
    - There was no user authentication or identification on a given system
    - Phone numbers were posted publicly to allow access into ARPANET for possible malicious intent

There was no network security and was known more as network insecurity. In order to

establish an effective environment that was secure, many changes needed to take place.

Developed by a task force within the DOD, the Rand Report R-609 was created to establish guidelines on security measures for resource-sharing computer systems. These general guidelines are meant to be flexible and not specific to one kind of system environment. Although geared towards government installations the report can be used in “civil” methods as well. Depending on the sensitivity and configuration of the data in a system would require different security measures. These guidelines cover the unexamined points described by Robert.

Remote sites having no protection from unauthorized remote users fall under:

**Part C - Technical Recommendations > IV. Access Control throughout the System > Information Access**

A user may be authorized to only specific areas of the computer system and unauthorized in others. Access privileges must be checked against the user to allow them access. Also if any information from a file is authorized to be sent to a user, then the remote terminal itself has to also be verified. In order to complete the request a computer would have to check an internal list that would hold all authorizations and verify against it.

**Part D - Management and Administrative Control > Terminal Control**

There are different procedures when using remote terminals such as logging when a user has been utilizing a terminal remotely. Also ensuring that the display of the terminal is erased of any classified information prior to next use, removing any hardcopies, and securing the terminal after its use during its shutdown phase.

Password format and structure issues fall under the following sections:

**Part B - Policy Considerations and Recommendations > II. System Personnel > System Security Officer**

The System Security Officer is important regarding password format and structure. He/she is responsible for establishing clearances for users and programs the security parameters into the system.

**Part C - Technical Recommendations > IV. Access control throughout the system > User Access**

States that passwords must be from an approved source or created and provided under the guidance of the System Security Officer using any approved methods. A user cannot generate their own passwords and must change their password regularly as stated by the providing source. If the level of classification is high then the user may need to authenticate many times.

Dial up connections lacking safety procedures fall under these categories:

**Part C - Technical Recommendations > VI. Terminals > Terminal Identification**

Any terminal that connects remotely to a resource-sharing system much get verified by that system via identification. The system should also be able to test the identification of the connecting terminal at any time.

**Part C - Technical Recommendations > IV. Access control throughout the system > User Access**

A password design has to be used if a terminal is connecting via dial up to provide authentication.

No user authentication or identification on any system has key point areas:

**Part B Policy Considerations and Recommendations > II. System Personnel > “User Authentication”**

Every user is required to verify him or herself and authenticate their identity to the system anytime it places a request. These methods will be adequate for protection of the system overall and assigned by the System Security Officer.

**Part B Policy Considerations and Recommendations > VI. Information Security Labels > “Information Output”**

Even though a user may or may not have clearance for sensitive information, a warning and/or request for authentication should be placed to allow the user access if they have the credentials. At the very least it will advise the level of classification.

In conclusion the Rand Report outlines the unexamined items prior to its creation and advises that every computer system design is different so one security format may not be adequate for another and should be planned out with the provided outline in mind. Physical security was not included as it was already established before the birth of ARPANET.