COIT20246 Networking and Cyber Security

Week 09 Tutorial Activities

Cyber Security Management

Aim to complete Tasks 1 to 3 during the tutorial. These tasks contribute to your project, so you may work in your project groups, but all students need to make contributions to their individual journals.

# Task 1. Select Security Objectives

Considering your Project, select four (4) different sub-categories of objectives from the NIST Cyber Security Framework. Select two (2) each from Protect and Detect functions, where both must be from different categories. That is:

* Function: Protect; Category: A; Sub-category: 1
* Function: Protect; Category: B; Sub-category: 2
* Function: Detect; Category: C; Sub-category: 3
* Function: Detect; Category: D; Sub-category: 4

For each objective selected, give a brief reason why it is important for your Project, and what attack/vulnerability it may mitigate.

In your journal:

* For each of the selected sub-categories, give the function, category, and sub-category, and then explain why it is important and explain an attack/vulnerability it may mitigate.

ANS:

As per the NIST Cyber Security Framework, I select Category A which covered access control protection that has anomalies and events detection function, and Category C which covered data security protection that has security continuous monitoring and detection process as a detection function. These categories have different function and protection for specific projects such as Access control protection involve limiting access to system and network and data security protection involves using security software to protect data and information.

Similarly, Category A (Access control) mainly enable an organization to manage who can authorize to access network and resources and who cannot that means this category mainly verify user access and control the access level that is granted to users. Access control is categorized into three such technical access control, physical, and administrative access control which have different functions over access resources and data. These 3 categories, it classifies into 6 sub-categories such as preventive, detective, deterrent, compensating, corrective, and recovery. Access control is important for the project because it mainly limits access to information and processing systems as well as protects resources against threats from intruders. Similarly, access control help to protect against unauthorized access vulnerability, DoS attacks, ransomware attacks, and other so where it limits user access and verifies the correct authorized users to access the resources and data within the network. Access control helps an organization mitigate the unauthorized vulnerability, dos attacks, and ransomware attacks from the network.

Similarly, Data security (Category C) mainly provides a function regarding safeguarding digital information and protecting data information from corruption, theft, and unauthorized access. Data security is categorized into four classifications such as public data security, internal-only data security, confidential data security, and restriction data security. Within these categories, access controls, authentication, encryption, backups ad recovery, data masking, data resiliency, and data erasure are the sub-categories of data security. Data security is important for the project because it provides safeguards to the digital information to protect that information from corruption, theft, and unauthorized access to hardware, software, storage device, administrative control system, or the organization's policy and procedures. Data security mainly protect data from accidental exposure, data breaches, Phishing attacks, other social engineering attacks, insider threats, ransomware attacks, and many more vulnerability and threats and also help an organization to mitigate by accepting integrity, confidentiality, and availability. Data security also provides data auditing, data alerts in real-time, data risk assessment, and many more data security technology.

# 

# Task 2. Create Asset Inventory

Re-visit Task 1 from Week 08 where you listed important assets for your Project. Expand on the assets to cover all asset types and specific assets. Use a table for each asset type (e.g., one table for Data assets, another table for Hardware assets). Include identifying information for the assets (you may make up fake values if unknown, e.g., MACs, serials). For the Data assets, include a classification based on value or access (or both), and identify the important protections, e.g., CIA (you identified some protections in Task 1 from Week 08).

In your journal:

* Tables of assets for the six (6) asset types, ensuring the Data assets also are classified.

ANS:

|  |  |  |  |
| --- | --- | --- | --- |
| **Assets types** | **Classification** | **Protection** | **Reason** |
| Security camera | Hardware assets | Availability | To record the availability if the camera is committed. |
| Firewall system | Hardware assets | Security system design | Filter the traffics and detect the malware as well as block unauthorized accesses. |
| Workstation | Hardware assets | Availability and integrity | Securely provide a working environment and is also used for verities project operations. |
| Personal detail | Data assets | Availability and integrity | Protect personal detail for users and organizations. |
| Financial management system | Data assets | Availability, confidentiality, and integrity | Secure financial records of individuals, only authorized users should access that information. |
| Application and database documents | Data assets | Availability, confidentiality, and integrity | Secure software applications and database system records and documents. |

# Task 3. Information Flow Check

For the two (2) most important Data assets identified in Task 1, draw an information flow diagram that identifies the connection between the Data asset and all other assets. Use the diagrams to confirm that your asset inventory is accurate (fix your inventory if you identify mistakes).

In your journal:

* Diagrams of information flow for two (2) important assets.

ANS:

Financial management system

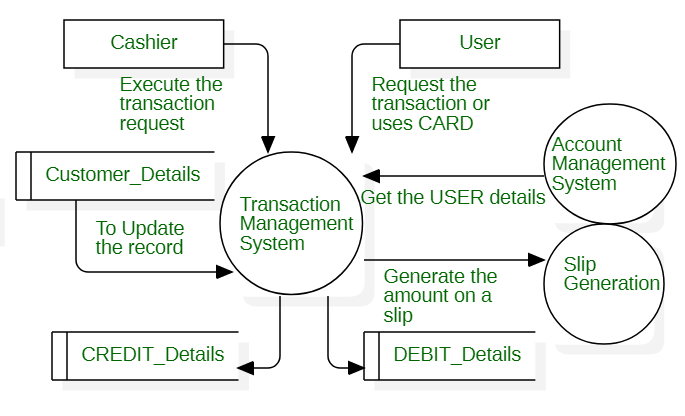


Figure : Data flow diagram for financial management system

Firewall Assets

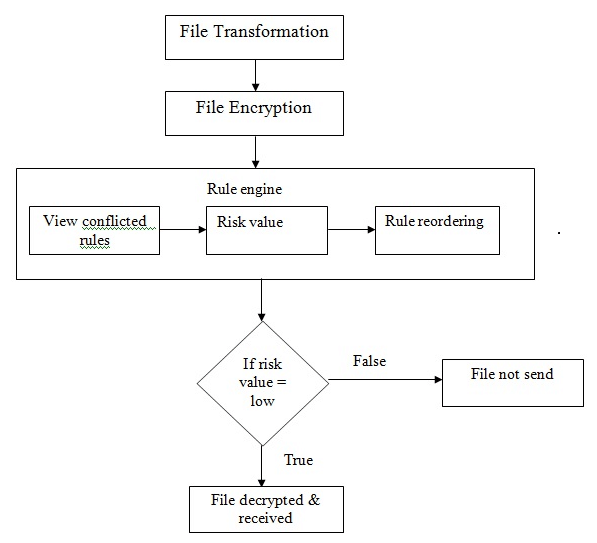


Figure : Data flow diagram for Firewall

# 

# Task 4. Conduct a Risk Analysis

Conduct a risk analysis for your Project, using the risk assessment template spreadsheet. There is no need to include this in your journal, as it will be in your project submission.

ANS:

Risk assessment help organization and employee process the assessment to review and evaluate their organizational risk. That means risk assessment defines the process of identifying the potential risk and hazards and analyzing those hazards if occur in the organization. It mainly determines the potential hazard and its impacts. To process the risk assessment, the following step should consider.

Step 1: Identify hazards and potential risks.

Step 2: Decided who might harm and how.

Step 3: Risk evaluation and precaution decided

Step 4: Record results and implement them in the business organization.

Step5: Review assessment and update (if necessary)

Risk analysis report for each asset

|  |  |  |  |
| --- | --- | --- | --- |
| **S. N** | **Assets** | **Threats** | **Priority** |
| 1. | Security camera | Hacked or leakage | High |
| 2. | Firewall system | DDoS attacks | Medium |
| 3. | Workstation | Phishing attacks | High |
| 4. | Personal detail | Data breaches | Medium |
| 5. | Financial management system | Malware | Medium |
| 6. | Application and database | Unauthorized access and DoS attacks | High |

Risk assessment template (Risk rating table)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Risk Value** | | | | |
| ***Risk Name*** | ***Likelihood out of 5*** | | ***Impacts out of 5*** | ***Risk rank out of 25*** |
| Hacked or leakage | 4 | 5 | | 20 |
| DDoS attacks | 3 | 4 | | 15 |
| Phishing attacks | 4 | 5 | | 20 |
| Data breaches | 4 | 5 | | 20 |
| Malware | 4 | 5 | | 20 |
| Unauthorized access | 3 | 4 | | 15 |
| DoS attacks | 3 | 4 | | 15 |
|  | 4 | 5 | | 20 |



Cyber Security Management 1