|  |  |  |
| --- | --- | --- |
| Name | FN: | Email: |
| Gennadiy Furduy | 1601321027 | gennadiy@furduy.com |

**UNWE – 2020, MS in CIP (Cybersecurity for CIP)**

|  |  |
| --- | --- |
| **Exercise Title** | Developing a Resilience Strategy  (INSTRUCTIONS) |
| **Objectives** | * Identify a service and related assets * Characterize the potential impact to the organization if one or more of the assets are disrupted. * Begin to develop resilience requirements for one of the assets. * Begin to develop a resilience strategy (a protection strategy and a sustainment strategy) for the asset to meet the resilience requirements |
| **Instructions** | To complete this exercise, perform the following tasks. These numbered steps correspond to the numbered circles on the following pages.  **Part 1: Exercise 3 – The building blocks of CERT-RMM**   1. Identify a service that is important in your organization. An example may be a support service (such as paying vendors) or an organization-specific service (such as producing widgets). Document the mission of the service and consider its strategic importance. 2. Identify and document four assets (a person, a piece of information, a technology component, and a facility) that are required by the service. Name the assets (such as “Joe Smith” or “medical records”). 3. Answer the questions about the importance of the service, potential disruptions to one of the assets, the impact to the service, and the impact to your organization.   **Part 2: Exercise 5A – Developing resilience requirements**   1. Select one of the assets from step 2 for requirements development (suggestion: select an information asset). 2. Describe some confidentiality requirements for the asset. 3. Describe some integrity requirements for the asset. 4. Describe some availability requirements for the asset.   **Part 3: Exercise 5B – Protecting and sustaining assets**   1. Copy the asset name from step 4 to the step 8 box. 2. Based on the resilience requirements you developed in part 2,    1. Document a protection strategy for the asset and describe the administrative, technical, and physical controls that would be necessary to implement the strategy and meet the stated requirements.    2. Document a sustainment strategy for the asset and describe the administrative, technical, and physical controls that would be necessary to implement the strategy and meet the stated requirements. Consider strategies to sustain the availability of the asset as well as strategies to   sustain the service in the absence of the asset. |

|  |  |
| --- | --- |
| **Service Name:**  Identity Service for banks | **Service Mission:**  Identification user and user role |
|  |  |  |  |
| Asset 1:  System Administrators,  Bank management | Asset 2:  User data, user role | Asset 3:  IdentityServer4 on dedicated server | Asset 4:  Datacenter |
| **People** | **Information** | **Technology** | **Facilities** |

|  |
| --- |
| A. What is the strategic importance of the service? |
| As IS provider, our main objective is to identify users who use bank system |
| B. Which asset could be disrupted and how? |
| User data and roles could be lost, corrupted or stolen |
| C. What would be the impact on the service mission if the asset were disrupted? |
| Users can’t have access to bank system or intruder will has access to banking information |
| D. What consequences, if any, would the organization experience? Consider a) reputational harm, b) impacts to life, safety, and health of employees and customers, c) legal fines or penalties, and d) other financial losses. |
| Serious reputational and financial harm |

|  |  |
| --- | --- |
| Select an asset from Step 2: | |
| User data, user role | |
| *Suggestion: select the information asset, identified in step 2.* | |
|  |  |
|  | ***Confidentiality:*** *Ensuring that only authorized people, processes, or devices have access to an information asset* |
| **Confidentiality requirements for the asset:** |
| User data and role may only be accessed by authorized bank officers. |
| *Example: Patient medical records may only be viewed by the patient’s doctor and medical staff expressly approved by the patient’s doctor.* |
|  |
| ***Integrity:*** *Ensuring that an asset remains in the condition intended and so continues to be useful for the purposes intended* |
| **Integrity requirements for the asset:** |
| User data and role may only be changed or added by bank management staff. |
| *Example: Patient medical records may be altered only by the patient’s doctor. Alterations approved by medical staff must be authorized by the patient’s doctor.* |
|  |
| ***Availability:*** *Ensuring that an asset remains accessible to authorized users (people, processes or devices) whenever it is needed* |
| **Availability requirements for the asset:** |
| User data and role must be available on demand, 24x7 |
| *Example: Patient medical records must be available to authorized personnel on demand, 7 days a week, 24 hours a day.* |

|  |
| --- |
| Asset from Step 4: |
| User data, user role |

|  |  |  |
| --- | --- | --- |
| **PROTECT** |  | **SUSTAIN** |
| **Based on the resilience requirements, the protection strategy for this asset is:** |  | **Based on the resilience requirements, the sustainment strategy for this asset is:** |
| The protection strategy for user data is to strictly limit viewing access to authorized staff and applications, modification access to bank management staff only. |  | The sustained strategy is to ensure that users, applications, and managers have access from every location through the Internet. |
| *Example:* *The protection strategy for patient medical records is to strictly limit viewing and modification access to authorized personnel.* |  | *Example: The sustainment strategy is to ensure that authorized medical personnel have access even if the original electronic paper records are unavailable.* |
| **The strategy would be implemented through these controls:** |  | **The strategy would be implemented through these controls:** |
| *Administrative:* |  | *Administrative:* |
| Create and enforce an access policy |  | Develop and maintain the continuity plan. |
| *Example: create and enforce an access policy* |  | *Example:* *develop, test and maintain continuity plans* |
| *Technical:* |  | *Technical:* |
| Require login/token for identification. Require biometric identification to access to data center. |  | Synchronize database to a redundant data center. Automatically backup data. |
| *Example: require ID/password to access electronic medical records, electronic IDs to access data center* |  | *Example: Scan all paper records for digital storage; synchronize electronic storage to redundant data center for failover; automatically backup data* |
| *Physical:* |  | *Physical:* |
| Lock data center and strictly limit access. |  | Physically separate primary and secondary data centers. Store backups offsite. |
| *Example: lock data center and strictly limit access* |  | *Example:* *physically separate primary and secondary data centers; store backups offsite* |