Cyber Security Assessment and Management Worksheet #2 – Risk Management

1. Organization you choose and respective assumptions

- A **hospital** was chosen for the risk assessment and here are the respective assumptions:

- The analysis is on a yearly basis
- The hospital operates 24/7, providing emergency services, surgeries, and patient care at all times
- There is an adequate supply of medical resources (medications, equipment, and supplies) available to meet patient demand
- The hospital has well-defined emergency protocols for handling pandemics and mass casualty incidents
- The hospital has weak cybersecurity measures to protect against ransomware attacks, data breaches, or unauthorized access to sensitive patient information
- Transport vehicles are driven by staff from the hospital
- The hospital is regularly victim of attempted Cyberattacks
- The video cameras are connected to the power of the building and they don't have failure protection mechanisms
- The hospital has steady financial resources, whether from patient fees, insurance claims, or government funding, to cover operational costs and potential emergencies
- The hospital does not have training programs to keep staff up-to-date on new procedures, technology and emergency protocols
- The hospital has a well-functioning access control system that handles staff permissions and the attendance register
- The backup databases are isolated from the normal databases, and only the person responsible for restoring the system has the authorization to access it

2. Information items included in #List 1

- **Infrastructure:**
  - **Buildings and Facilities**:
    - Main hospital building, outpatient clinics, specialized departments (ICU, emergency rooms, operating theaters, labs)
    - Parking facilities, storage units, and medical waste disposal areas
  - **Medical Equipment**:
    - Diagnostic machines (CT scanners, X-ray machines, ultrasound equipment)
    - Treatment equipment (ventilators, dialysis machines, anesthesia machines)
    - Surgical tools and instruments
    - Patient beds, stretchers, wheelchairs
  - **Non-Medical Equipment**:
    - HVAC systems, elevators, generators, fire safety systems
    - Office equipment (desks, chairs, printers, copiers)
  - **Vehicles**:
    - Ambulances and other hospital-owned transport vehicles
- **Technological infrastructure:**
  - **Information Systems:**
    - Electronic Health Records (EHR) systems for patient data
    - Hospital Management Software (for billing, scheduling, and resource management)
    - Pharmacy management systems
  - **Communication Networks:**
    - Internal communication systems (telephones)
    - Hospital Wi-Fi and intranet
    - Network servers, routers
  - **Backup and Data Storage:**
    - Data centers and cloud storage systems
    - Backup power systems
- **Employee information:**
  - **Medical Staff:**
    - Doctors, surgeons, nurses, and specialists
    - Pharmacists, laboratory technicians, paramedics
  - **Administrative and Support Staff**:
    - Hospital administration (managers, HR, finance personnel)
    - IT staff (network administrators, cybersecurity teams)
    - Maintenance and housekeeping staff
    - Security personnel
- **Financial/insurance and business planning data:**
  - **Financial Data:**
    - Patient billing information, insurance claims, accounts receivable/payable data
    - Budgets and financial statements
    - Endowments, grants, and donations (funding sources)

- **Contracts:**
  - Supplier contracts (medical equipment, drugs, and consumables)
  - Service provider contracts (IT services, janitorial, waste disposal)
- **Public Data and presence on social media:**
  - **Website:**
    - Official hospital website that contains important public-facing information such as services offered, contact details, staff directories, and patient resources
    - Online appointment booking systems or patient portals
    - Content management systems (CMS) that handle the hospital's online presence
  - **Publicly Available Information**:
    - Data on hospital performance, quality ratings, or accreditations that might be published by external bodies or government entities
    - Published research and medical studies by hospital staff available in the public domain
  - **Social Media Accounts and Media Content:**
    - Hospital's official accounts on social platforms like Facebook, Twitter, Instagram, LinkedIn, YouTube, and any other relevant platforms
    - Social media campaigns promoting services, health tips, or awareness events
    - Blogs, articles, health tips, and updates shared by the hospital
    - Videos and images related to hospital services or medical advice