There are different model of cybersecurity architecture. For SecureGov Ministries we selected "Layered defense" to protect systems, networks, and information.

Concept of Layered Defense

Definition: The **Layered Defense model**, is a comprehensive cybersecurity strategy that employs multiple layers of security controls to protect information and systems. The idea is to create a series of defensive mechanisms so that if one layer fails, others will still be in place to thwart an attack.

Concept: The idea is to implement multiple layers of security controls and safeguards. Each layer provides protection against different types of threats, so even if one layer fails, others are in place to mitigate the risk. It is often about the number and types of barriers or security measures, focusing on technical aspects.

Application: This strategy is often visualized as a series of concentric circles, where the innermost circle is the most valuable asset. Each layer must be breached before the asset can be reached.

Here’s a breakdown of the key components:

1. **Physical Security**:
   * **Controls**: Security cameras, access control systems, biometric scanners, and physical barriers.
   * **Purpose**: Prevent unauthorized physical access to facilities and hardware.
2. **Network Security**:
   * **Controls**: Firewalls, intrusion detection/prevention systems (IDS/IPS), and secure network architecture.
   * **Purpose**: Protect the network infrastructure from unauthorized access and attacks.
3. **Endpoint Security**:
   * **Controls**: Antivirus software, endpoint detection and response (EDR) solutions, and device encryption.
   * **Purpose**: Safeguard individual devices from malware and other threats.
4. **Application Security**:
   * **Controls**: Secure coding practices, application firewalls, and regular security testing.
   * **Purpose**: Ensure that applications are free from vulnerabilities and resistant to attacks.
5. **Data Security**:
   * **Controls**: Data encryption, data loss prevention (DLP) tools, and secure data storage.
   * **Purpose**: Protect sensitive data from unauthorized access and breaches.
6. **Identity and Access Management (IAM)**:
   * **Controls**: Multi-factor authentication (MFA), role-based access control (RBAC), and single sign-on (SSO).
   * **Purpose**: Ensure that only authorized users have access to systems and data.
7. **Security Monitoring and Incident Response**:
   * **Controls**: Security information and event management (SIEM) systems, continuous monitoring, and incident response plans.
   * **Purpose**: Detect and respond to security incidents in real-time.
8. **User Education and Awareness**:
   * **Controls**: Security training programs, phishing simulations, and awareness campaigns.
   * **Purpose**: Educate users about security best practices and how to recognize potential threats.

The **Layered Defense model** is effective because it doesn’t rely on a single point of failure.