**📘 Summary: 02 Cybersecurity Functions**

**1. Purpose and Scope of Cybersecurity Functions**

* Provides a **structured approach** to managing enterprise cybersecurity.
* Aligns technical and non-technical **capabilities** to business needs.

**2. Enterprise Security Architecture – Functional Areas**

* **Network Security**:
  + - * Controls for data flow (e.g., firewalls, proxies, VPN).
* **Infrastructure Security**:
  + - * Protects IT components (servers, desktops, mobile).
* **Application Security**:
  + - * Controls for software, SDLC, APIs.
* **Data Security**:
  + - * Controls for storage, classification, and handling of data.
* **User Security**:
  + - * User behavior, malicious threats.
* **Cyber Defense**:
  + - * Monitors and manages control effectiveness.
* **Cybersecurity Governance**:
  + - * Oversight, strategic alignment, measurement.
* **Risk Management**:
  + - * Identifies, captures, and mitigates risk.

**3. Cybersecurity Operating Model**

* **Operational Capabilities**:
  + - * Daily management of security services.
* **Non-Operational Capabilities**:
  + - * Development, awareness, training, risk management.
* **Governance Interface**:
  + - * Oversight of both areas, links to the business.
* **HR & Facility Security**:
  + - * Often separate, but related.

**4. Organisational Interfaces**

* **Cybersecurity interfaces with multiple enterprise functions:**
  + Business
  + IT (Infrastructure, Apps, Networks)
  + Cloud, HR, Audit, 3rd Parties

**5. Roles & Responsibilities – RACI Model**

* **Responsible**
  + - Does the work.
* **Accountable**
  + - Owns the outcome.
* **Consulted**
  + - Provides input.
* **Informed**
  + - Kept up-to-date.
* **Clear definitions**
* Critical during incident handling, audits, and operations.

**6. Cybersecurity Function: Network Security**

* Focuses on network devices/configuration (IDS/IPS, Firewalls, WAF, Proxies, etc.)
* Covers both **on-prem** and **cloud** environments.
* **Processes**:
  + - * Config hardening
      * Rule review & approval
      * SIEM/SOC integration
      * Audit & incident support

**7. Cybersecurity Function: Infrastructure & Application Security**

**Infrastructure Security**

* **Covers**:
  + Servers, Desktops, Mobile Devices, IoT, Cloud platforms
* **Processes**:
  + PKI, EDR, Anti-malware
  + Directory services, Certificates
  + Mobile device management

**Application Security**

* Involves:
  + Secure SDLC, API security, SAST, SCA
* **Processes**:
  + Compliance with security requirements
  + Testing & governance integration

**8. Cybersecurity Function: Identity and Access Management (IAM)**

* Manages access to resources by all types of users.
* **Processes**:
  + Joiners/Movers/Leavers
  + Directory & group management
  + Federation (SSO)
  + Recertification
  + PAM onboarding

**9. Cybersecurity Function: Data Security**

* Covers data throughout its lifecycle (classification, discovery, storage, disposal).
* **Processes**:
  + DLP
  + Removable media control
  + Data retention & disposal
  + Privacy & compliance support

**10. Cybersecurity Function: Threat & Vulnerability Management (TVM)**

* Manages threats and vulnerabilities using:
  + Scanning, intelligence, hunting
* **Processes**:
  + Vulnerability scanning & analysis
  + Remediation tracking
  + Threat advisory monitoring

**11. Cybersecurity Function: Security Monitoring**

* **SIEM** implementation and monitoring
* Alert triaging and integration of threat intelligence
* **Processes**:
  + Use case development
  + Alert analysis and reporting
  + Automation and IR integration

**12. Cybersecurity Function: Incident Response**

* Ensures **effective reaction** to security incidents.
* **Processes**:
  + Investigation, containment, recovery
  + Evidence preservation
  + Lessons learned
  + IR simulations