Cybersecurity for Dummies

Chapter 1: What Exactly Is Cybersecurity?

- **Cybersecurity definition**:
  The practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks.
  ⚡ Note: Broader than just "IT security"; includes people, processes, and tech.

- **The CIA Triad**:
  1. **Confidentiality** → Only authorized access (e.g., encryption, access controls).
  2. **Integrity** → Data must be accurate and trustworthy (checksums, hashing).
  3. **Availability** → Systems and info available when needed (redundancy, backups).

- **Security layers**:
  1. **Technology** (firewalls, antivirus, intrusion detection).
  2. **People** (user training, awareness).
  3. **Processes** (policies, incident response plans).
- **Why this matters for SBD**:
  Security is not just a "tool" — it's a **philosophy** that guides how systems are built.

Chapter 2: Getting to Know Common Cyberattacks

- **Malware**:
  - **Viruses** → Attach to programs/files, spread when executed.
  - **Worms** → Self-replicating, spread without human action.
  - **Trojans** → Disguised as legitimate software.
  - **Ransomware** → Encrypts data and demands payment.
  - **Spyware/Keyloggers** → Steal data silently.
- **Phishing**:
  - Fake emails/websites to trick users into giving credentials.
  - Still the **#1 attack vector** due to human weakness.
- **DoS/DDoS**:
  - Flood a system with traffic to shut it down.
  - Example: Mirai botnet using IoT devices.
- **SQL Injection**:
  - Attackers exploit poorly validated inputs to access/modify databases.
- **Man-in-the-Middle**:
  - Attacker intercepts communication (e.g., insecure Wi-Fi hotspots).
- **Lesson for SBD**:
  Most attacks exploit **design flaws** (weak validation, insecure defaults, poor resilience).
  → If systems are secure by design, these vectors are harder to exploit.

Chapter 3: Bad Guys and Accidental Bad Guys

- **Who are the attackers?**
  - **Cybercriminals** → Financial motives (credit card theft, ransomware).
  - **Hacktivists** → Political/social motives (Anonymous, WikiLeaks leaks).
  - **Nation-states** → Espionage & cyber warfare (Stuxnet, Russian hacks).
  - **Insiders** → Employees (either malicious or careless).
- **Accidental "bad guys"**:
  - Weak passwords, clicking malicious links, misconfigurations.
  - Example: Healthcare staff emailing patient data to wrong person.

- **Why this matters for SBD**:
  - Humans are often the **weakest link**.
  - Designing systems with **usability + security** (e.g., password managers, MFA prompts) reduces human error.

Big Picture Takeaways

1. **Cybersecurity for Dummies** gives you the *landscape*: what cybersecurity is, the main attacks, and who the attackers are.
2. **Calder's Essential Principles** gives you the *professional framework*: laws, governance, vulnerabilities, and practical defences.
3. Together they show: Cybersecurity is about **anticipating risks** and **embedding defences into design** — the very essence of *Secure by Design*.