Cyber Security: Essential Principles to Secure Your Organisation

Chapters 1 & 2 (Calder, 2020)

Chapter 1 – Information Security vs Cybersecurity

- **Information Security**: Protecting *all* information (paper + digital).
- **Cybersecurity**: Focus on *digital/electronic* information.
- **Laws & Regulations**:
    - **GDPR** (EU) → strict privacy, up to €20m fines.
    - **CCPA** (California) + **LGPD** (Brazil) → user consent + transparency.
    - **NIS Directive** → continuity for critical services.
    - **PCI DSS** → credit card payment security.
- **Takeaway**: Security is not optional; it's now enforced by law & contracts.

Chapter 2 – Threats and Vulnerabilities

- **Risk = Threat × Vulnerability**.
    - Threat: malicious actor or natural event.
    - Vulnerability: weakness that can be exploited.
- **Examples**:
    - SQL injection → poor coding practices.
    - Unpatched systems → outdated software.
    - Leaky roof in server room → physical + environmental vulnerability.
- **Types of Malware**:
    - Viruses, worms, Trojans, ransomware, hybrids, fileless malware.
    - WannaCry = worm + ransomware.
    - Stuxnet = worm targeting Iranian nuclear systems.
- **Hackers**:
    - Script kiddies (low skill, using pre-built tools).
    - Blackhats (skilled, exploit zero-days).
    - Hacktivists (political/social motives).
    - Nation-states (espionage & infrastructure attacks).
    - Ethical hackers (pentesting, prevention).
- **Defences**:
    - Awareness training.
    - Patch management.
    - Antivirus/firewalls.
    - Secure configuration (disable defaults, segment networks).
    - Penetration testing.

    - Backups (ransomware defence).
- **SBD focus**:
    - **Build with resilience in mind** → Secure defaults, patching, separation of duties.
    - Security should be **proactive, not reactive**.

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*.