CHAPTER 15

CYBERSECURITY & INFORMATION SECURITY RISKS

Cybersecurity is the **cornerstone of trust, reliability and resilience** in the digital age. Covers its **foundations & evolution**, major **threats**, **real-world breaches**, **defence strategies**, risks from **AI, IoT & cloud**, advanced technologies, **best practices** and the **cyber-talent shortage**.

CHAPTER ROADMAP

1. Foundations of cybersecurity
2. Major cybersecurity threats
3. Real-world incidents: lessons
4. Strategies for defence
5. Emerging risks — AI · IoT · cloud
6. Advanced technologies
7. Best practices
8. Shortage of cyber resources

DEFINITION

Cybersecurity is the practice of protecting computer systems, networks, software and data from digital threats, unauthorised access and malicious attacks.

Ensures the **integrity, confidentiality and availability** of digital assets, involving both **human users** and **technology**. Applies to business, government, healthcare and personal devices.

Confidentiality (C)
Only authorised people see the data.

Integrity (I)
Data stays accurate and unaltered.

Availability (A)
Systems keep running without disruption.

1.2 Evolution from the Internet's Origins

Military research mid-20th c.	Isolated computers	PCs · mobile · IoT	Cloud & remote work

Each step **expanded the attack surface** — today's solutions must secure **centralised and decentralised** environments.

1.3 Why it's a top business risk

- **Dependence on technology** — a breach halts core functions
- **Sophisticated attackers** — AI-driven malware, state-sponsored hackers
- **Sensitive data everywhere** — prime targets
- **Remote work & cloud** — bigger attack surface

A successful attack can cause

Financial loss · **Reputational damage** · **Regulatory penalties** · **Operational disruption**

Laws & Standards

Global: GDPR (EU) · **CMMC** (USA) · NIST CSF (USA) · ISO/IEC 27001 · FATF guidance on virtual assets & cybercrime
Pakistan: PECA 2016 · SBP Enterprise Technology Governance Framework · SECP Cybersecurity Guidelines · Cyber Security Policy (2021)

2 MAJOR CYBERSECURITY THREATS

systems · networks · human behaviour

2.1 Malware — infiltrates without the user's knowledge

Adware
Floods users with **unwanted ads**; may slow systems or lead to malicious sites.

Spyware
Covertly collects credentials, browsing history, financial data.

Virus
Attaches to legitimate software; spreads & corrupts files.

Worm
Self-replicates across networks without user action; consumes resources.

Trojan Horse
Disguised as legitimate software; creates **backdoors**.

Scareware
Tricks users into thinking they're infected → buy **fake software**.

2.2 Cybercrime Varieties

Cyberstalking	Online harassment / intimidation
Forgery	Counterfeit digital documents
Software piracy	Unauthorised copying of copyrighted software
Cyberterrorism	Attacks on critical infrastructure for political / ideological aims
Phishing	Fraudulent messages to steal info
Hacking	Unauthorised system access
DoS / DDoS	Traffic overload → unavailable to users

2.3 Sophisticated Attacks

Salami attack	Steal **tiny amounts** over time to avoid detection
Data diddling	**Alter data before processing** → wrong outputs
Email spoofing	**Fake sender address** looks trusted
Logic bomb	Code **triggered by an event** (update, user action)

2.4 Insider vs External

Insider
Employees/contractors — **malicious** (leak for gain) or **unintentional** (negligence)

External
Cybercriminals to **state-sponsored** attackers — malware, phishing, **APTs**

3 REAL-WORLD CYBERSECURITY INCIDENTS

what failed → the lesson

Incident	What happened	Weakness exploited	Lesson
Equifax (2017)	Data of ~**147m** Americans stolen; settlement > **$700m**; executives resigned	Known but **unpatched Apache Struts** flaw; poor asset inventory	**Timely patch management** & internal controls
Target (2013)	Card data of **40m+** customers; > $200m costs	Stolen credentials of a **third-party HVAC vendor**; moved laterally to POS	**Third-party risk**, network segmentation, access control
WannaCry (2017)	Ransomware in **150+ countries**; UK **NHS** surgeries cancelled	**EternalBlue** SMB flaw — patch existed but not applied	Update **outdated software**; ransomware preparedness
Colonial Pipeline (2021)	US fuel shortages; **$4.4m** ransom (part recovered)	Legacy **VPN account without MFA**	Secure remote access; **MFA**; critical-infrastructure readiness
Bangladesh Bank (2016)	~$1bn fraudulent **SWIFT** transfers; **$81m** stolen	Weak endpoint security, no intrusion detection, little segmentation	Endpoint security, IDS, segmentation

Recurring vulnerabilities

Poor patch management · Unsecured third-party access · Outdated systems · No network segmentation · Weak authentication

Also shows the need for **incident response plans & continuous monitoring**. Cybersecurity must be a **strategic business priority** backed by governance, investment and a **security culture**.

MEMORY HOOK Equifax & WannaCry = **Patch** · Target = **Vendor** · Colonial = **MFA** · Bangladesh = **SWIFT / segmentation**.

4 STRATEGIES FOR CYBERSECURITY DEFENCE

prevention · detection · response · automation

4.1 Prevent › 4.2 Detect & Monitor › 4.3 Respond › 4.4 Automate › 4.5 MSSPs

4.1 Preventive — Authentication

First line of defence: verify identity. Usernames & passwords → **2FA** (OTP via SMS/app) → **biometrics** (fingerprint, face, retina — finance, healthcare) → **MFA** combining them.

1K SYMMETRIC ENCRYPTION
one shared key

Same key encrypts & decrypts. **Fast** — good for large data **at rest** (databases, backups, cloud). **AES-256** most widely used.

Challenge: sharing the key securely — if intercepted, encryption fails.

2K ASYMMETRIC ENCRYPTION
public + private key

Public key encrypts, **private key decrypts** — no secret key to share. A sends to B using **B's public key**; only **B's private key** opens it.

Used for digital signatures, secure email, **SSL/TLS**. Algorithms: **RSA, ECC**.

Digital Certificates & HTTPS

A **digital certificate** binds a public key to a **verified identity**, issued by **Certification Authorities (CAs)** — DigiCert, GlobalSign, Let's Encrypt, Sectigo.
HTTP = plain text (interceptable). **HTTPS** = SSL/TLS encryption (padlock) → stops **man-in-the-middle** attacks.
The **handshake** uses **asymmetric** encryption to exchange a **session key**, then **symmetric** for speed.

Firewalls

Barrier between trusted & untrusted networks, filtering by rules. **NGFWs** add **IPS** & **deep packet inspection**, inspect encrypted traffic. **Host-based** protects a device; **network-based** protects the network.

4.2 Detection & Monitoring

Antivirus / Anti-malware

Signature-based (known) + **heuristic** (behaviour) detection; real-time & scheduled scans; ML for zero-days.

IDPS

IDS detects & **alerts**; **IPS** automatically **blocks**.

SIEM

Aggregates & **correlates** logs from firewalls, IDS, antivirus → full security view.

SOC

Security Operations Centre — **24/7** monitoring, detection & response (in-house or outsourced); uses SIEM, EDR, threat feeds.

4.3 Incident Response

- **Forensic analysis** — root cause, extent, attacker's footprint; AI forensics
- **Recovery plans** — isolate, restore from backups; **BCP & DRP**; automated failover
- **Post-incident analysis** — update policies & plans

4.4 Automated Security

- **Standardised protocols** — scans, config management, **self-healing** systems
- **Continuous monitoring** — AI flags e.g. surge in outbound traffic (exfiltration); behavioural analytics
- **SOAR** — Security Orchestration, Automation & Response: quarantine, forensics, notify, block — **no human needed**

4.5 What are MSSPs?

Managed Security Service Providers — third-party firms delivering **outsourced monitoring, management & response**; experts, tools, 24/7 cover too costly in-house (esp. SMEs).

Why MSSPs matter

24/7 monitoring
Rapid response

Expertise
Cross-industry teams

Cost efficiency
No full in-house SOC

Scalability
Grows with the business

Compliance support
ISO 27001, GDPR, NIST, PCI DSS

Services offered by MSSPs

1. SIEM monitoring
2. IDPS
3. Threat intelligence & IR
4. Vulnerability & patch oversight
5. Firewall & endpoint mgmt
6. Data Loss Prevention
7. Cloud security monitoring
8. Compliance reporting & advisory

Lets businesses focus on **core operations**; eases the **skills shortage**.

5 EMERGING CYBERSECURITY RISKS

AI · IoT · cloud

5.1 AI Risks

Risks: algorithmic bias (hiring, lending) · **black box** — no transparency · unethical uses (**deepfakes**, weapons, surveillance) · **over-reliance** on autonomous AI

Mitigate: audits & bias detection · ethical AI guidelines · **human oversight** · **Explainable AI (XAI)**

5.2 IoT Risks

Risks: weak device security (**default passwords**, no encryption) · bigger **attack surface** · data privacy · **botnets** — e.g. **Mirai** launched massive DDoS

Mitigate: network segmentation · device encryption · **firmware updates** · strong authentication / MFA, change defaults

5.3 Cloud Risks

Risks: misconfigured settings (public buckets, open ports) · lack of visibility (multi/hybrid) · **shared responsibility** gaps · breaches & insiders

Mitigate: CASBs · multi-cloud governance · configuration audits (AWS Trusted Advisor, Azure Security Center) · encryption & access control

6 ADVANCED TECHNOLOGIES IN CYBERSECURITY

Decoy Systems (Honeypots)

Intentionally vulnerable systems that attract attackers to **study their methods**. Widely used in **industrial control systems** (power grids, plants).

Automated Defences

Standardised protocols (scanning, patching, config monitoring); **scalable**; **self-healing** systems fix issues automatically.

Digital Signatures

Cryptographic proof of **authenticity & integrity** — **not** a scanned handwritten signature. Vital in legal & financial deals.

Smartphone Security

Encryption apps, **VPNs** (public Wi-Fi), biometrics; privacy tools like **face-blurring** apps.

7 BEST PRACTICES FOR CYBERSECURITY

Layered Security

Defence in depth: encryption (AES), NGFW with **DPI & IPS**, SIEM + IDS monitoring.

User Education

Phishing simulations · password managers & MFA · secure devices (VPN, no public Wi-Fi).

Automation

Vulnerability scanning · **patch management** · incident response automation.

Compliance

Follow legal & regulatory standards.

Proactive Defence

Threat intelligence · real-time monitoring · frequent risk assessments.

8 SHORTAGE OF CYBERSECURITY RESOURCES

millions of roles unfilled

Why the shortage?

- Rapid digital transformation (cloud, remote, IoT)
- Evolving threat vectors
- Lack of specialised training
- High **burnout & attrition**

→

How companies respond

1. **Upskill** staff (CISSP, CISM, CEH)
2. **Managed security services**
3. **AI & automation**
4. **Public-private partnerships** (boot camps, scholarships)
5. **Inclusive hiring** & flexible work

EXAM FOCUS · MCQ TRAPS

commonly confused points

1 Virus vs worm
Virus attaches to software; **worm self-replicates without user action**.

2 Trojan vs scareware
Trojan = disguised software opening a **backdoor**. Scareware = fake infection alert to sell software.

3 Salami vs data diddling
Salami = **small thefts over time**. Diddling = **altering data before processing**.

4 Logic bomb
Triggered by a **specific event** — not self-replicating.

5 Symmetric vs asymmetric
Symmetric = 1 shared key (AES, fast). Asymmetric = public/private pair (RSA, ECC).

6 Which key decrypts?
Encrypt with the **recipient's public key**; decrypt with the **recipient's private key**.

7 IDS vs IPS
IDS **alerts**; IPS **blocks** automatically.

8 SIEM vs SOAR vs SOC
SIEM = correlate logs. SOAR = **automated response**. SOC = the **24/7 team/unit**.

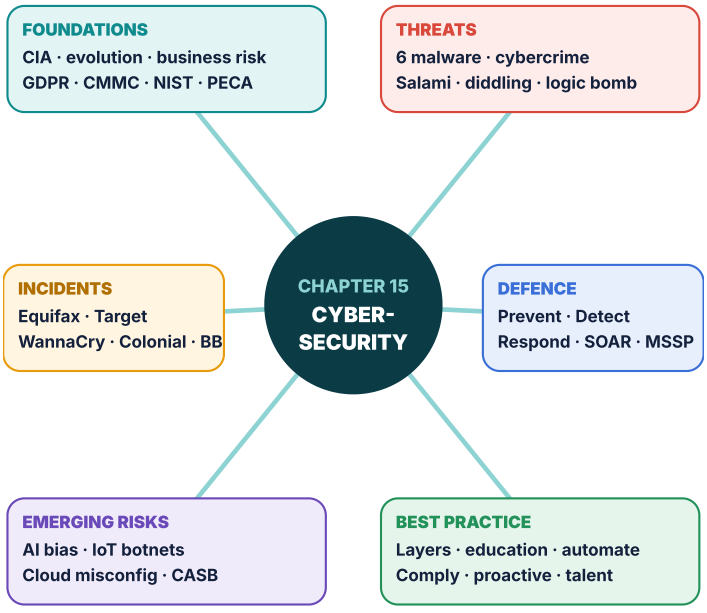
9 Honeypot
Deliberately vulnerable **decoy** to study attackers.

10 Cloud shared responsibility
Security split between provider & customer — misunderstanding leaves gaps.

CLASSIFY IT

1	Spreads across network alone	Worm
2	Rounding off cents into own account	Salami attack
3	Fake "CEO" email address	Email spoofing
4	Code runs on payroll date	Logic bomb
5	Target breached via HVAC vendor	Third-party risk
6	Auto-quarantine without humans	SOAR
7	Mirai hijacks cameras for DDoS	IoT botnet
8	Can't explain AI loan rejection	Black box → XAI

REVISION MAP



Protect CIA
Confidentiality, integrity, availability.

Know threats
Malware, cybercrime, insiders, APTs.

Learn lessons
Patch, MFA, vendors, segmentation.

Defend
Encrypt, firewall, IDPS, SIEM, SOC, SOAR.

Sustain
Layers, training, MSSPs, close talent gap.