OUTCOME 3 REMINDERS

Lecturer: Mark Gillan

IDENTITY, BIOMETRICS, TRAINING

- Types
- Pros/Cons
- Best for organisations to consider
- Training requirements
- Staff
- Visitor awareness
- Wi-Fi awareness and segregation

USE OF BIOMETRICS

Fingerprint:	• **Pros:** Low cost, fast. • **Cons:** Susceptible to environmental factors (dirt, moisture) and spoofing with latent prints.
Facial Recognition:	• **Pros:** Contactless, good for rapid authentication. • **Cons:** Affected by lighting, angle, and can be spoofed by high-resolution photos/masks.
Iris/Retina Scan:	• **Pros:** Extremely unique and highly accurate. • **Cons:** High cost, slower process, user acceptance issues.

ORGANISATIONAL USE OF BIOMETRICS

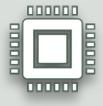
Discussion of what is best for Data/Organization Size:

Fingerprints are good for small to medium businesses for general laptop/device access (low cost, high volume).

Iris scans are typically reserved for highly secure areas or critical data access (e.g., financial systems, research labs) in larger organizations due to the high cost and accuracy.

PROTOCOLS / LEGALITIES

Security Focus: When sending sensitive biometric data (or its derived mathematical template) across a network like Wi-Fi, it must be encrypted.



This is typically done using **TLS/SSL** (Transport Layer Security) to prevent eavesdroppers from stealing the data in transit.

Legal Focus: In the UK and EU, adherence to the General Data Protection Regulation (GDPR) is paramount.

Biometric data is considered **special category data** (highly sensitive) and requires a higher level of protection, clear purpose, and often explicit consent from the user before processing.

BUILDINGS AND PREMISES

- Security Guards, CCTV
- Motion Detection Sensors, Heat & Fire Sensors
- Physical Barriers such as mantraps, doors, locks, partitions, sliding or rolling doors, fire doors, enclosures
- Fire detection, H&S inspections
- Biometric Access
- Cable locks, passwords, screen locks
- Training and testing, ICT maintenance
- Security slots and keeping / maintaining data backups offsite

TRAINING REQUIREMENTS

Staff Training:

- Must be mandatory and recurrent (e.g., quarterly)
- Key topics include Phishing and social engineering awareness
- Password hygiene (complexity, management)
- Clean Desk Policy
- Incident reporting procedures (who to call when a security event happens)

Visitor Awareness:

- Should include clear procedures for visitor logging/escorting
- Visible signage about restricted areas
- Ensuring Wi-Fi access is on a segregated guest network with no access to internal resources.

FIREWALL CONFIGURATION

- **Whitelist** (or 'allow list') is like a list of *only* permitted individuals—if you're not on the list, you're denied access by default.
- Whitelist is the most secure approach, following the principle of least privilege. Think of DENIAL.
- **Blacklist** (or 'deny list') is a list of *only* prohibited individuals (e.g., known troublemakers).
- For a blacklist, everyone *not* on the blacklist is allowed in by default. Think of ALLOWING.

PROS/CONS WHITELISTS AND BLACKLISTS

- **Example Whitelist:** Allowing only traffic related to secure web browsing (HTTPS) and company email.
- **Whitelisting** is safer but requires more ongoing effort to manage exceptions.

- **Example Blacklist:** Blocking access to a known list of malicious websites or competitor servers.
- **Blacklisting** is easier to set up but inherently riskier as it only blocks *known* threats, leaving the door open to new ones.

ACCESS CONTROL / PERMISSIONS

- **How it's done:** You use **NTFS Permissions** (New Technology File System) in Windows 11. This lets you decide exactly which *users* or *groups* can do what with a file or folder.
- **Step-by-step hint:** Right-click the file/folder → **Properties** → **Security** tab → **Edit** or **Advanced**.
- Key permissions are:
  - **Full Control** (can do anything, including deleting or changing permissions)
  - **Modify** (can read, write, and delete files/folders)
  - **Read & Execute** (can open and run)
- Remember, if you explicitly **Deny** someone a permission, it **always overrides** any Allow setting.

PHYSICAL SECURITY

- **Servers/Cabinets:** These must be kept in locked server cabinets (racks) within a secure room with physical access control (e.g., key card or biometric readers)
- Environmental controls, such as air conditioning (to prevent overheating) and fire suppression systems, are also essential.
- Maintenance to avoid hardware and software failures, including updating and patching plus regular inspection / reporting.
- **Laptops/Mobile Devices:** Enforce device encryption (like BitLocker) and use physical security devices (Kensington locks) in shared spaces.
- Staff must adhere to a clean desk policy to prevent sensitive information from being left exposed.

BACKING UP AND RECOVERY

- **Backup Process (Hint):** Windows offers tools like File History (for continuous backup of personal files) and System Image Backup (a complete snapshot of the entire C: drive).
- Most users now rely on OneDrive syncing for documents and photos as a simple, integrated backup.
- **Pros/Cons vs. Third-Party:**
- Windows tools are free, integrated, and simple for basic user needs.
- Third-party software (e.g., Veeam, Acronis) offers more efficient storage (better compression/deduplication), faster backups, and advanced features like backing up specific applications (application-aware backups) and reminders.

TYPES OF BACKUPS

Full: Copies all the selected data every time it runs.

Pros: The fastest and simplest to restore (you only need one file).

Cons: Takes the longest to run and uses the most storage space.

Differential: Copies all data that has changed since the *last full* backup.

Pros: Faster than a Full backup. Restoration requires only the *last Full* backup and the *latest Differential* backup.

Cons: The file size gets larger and larger until the next Full backup is taken.

Incremental: Copies all data that has changed since the *last backup* of *any* type (Full or Incremental)

Pros: The fastest type of backup to run and uses the least storage.

Cons: Restoration is the most complex, potentially requiring the *last Full* plus *every single Incremental* backup taken since.

IMPORTANCE OF TESTING RESTORE

Why Test?

- A backup that fails to restore is worthless.
- You must routinely test the restore process to ensure the data is not corrupted and that the process works within your time limits (RTO – Recovery Time Objective being maximum permissible downtime).

Pitfalls & Avoidance:

- **Pitfall:** Backups fail silently, or the files are corrupted.
- **Avoidance:** Verify the backup integrity using the software's features (checksums) and perform regular spot-checks (restoring a random file or folder) to a test location.

TIMINGS OF BACKING UP

RPO vs. RTO:

- You need to define your **Recovery Point Objective (RPO)**—the maximum acceptable data loss (e.g., 4 hours of transactions lost)—determines how often you back up.
- You also define your **Recovery Time Objective (RTO)**—the maximum acceptable downtime—determines how fast you need to be able to restore.

Hint: Backups should run outside of peak business hours (e.g., overnight) to minimise impact on network speed and system performance.

For critical systems, however, you may need near-continuous replication to achieve a very low RPO.

RAID

Redundant Array of Independent Disks

RAID is a technology that combines multiple physical hard drives into a single logical unit.

Used to improve performance or provide redundancy (fault tolerance)—meaning if one drive fails, the system keeps running and data isn't lost.

Think of it as teamwork for hard drives.

See next page for different RAID explanations...

RAID Type	What It Does (The Analogy)	Pros (Benefits)	Cons (Drawbacks)	Best Use Case
RAID 0 (Striping)	**The Speed Racer:** Data is split into pieces and written across two or more drives simultaneously.	**Fastest performance** (read and write) because multiple drives work at once.	**No redundancy.** If *any* single drive fails, **all data is lost**.	Video editing or high-performance gaming systems where speed is vital and data can be easily replaced.
RAID 1 (Mirroring)	**The Bodyguard:** All data is written identically (mirrored) onto at least two separate drives.	**Highest redundancy.** The system can survive **one drive failure** with no downtime.	**High cost.** You only get **half** the total drive space (e.g., two 1TB drives gives you 1TB of usable space).	Critical small servers, accounting data, or operating systems where **uptime is key**.
RAID 5 (Striping with Parity)	**The Smart Worker:** Data is striped across three or more drives, and a separate mathematical check (parity) is also spread across the drives.	**Good balance** of speed, storage capacity, and redundancy. Can survive **one drive failure**.	**Slower write speed** than RAID 1 or 0 due to the parity calculation.	General-purpose file and application servers in most medium-sized organisations.
RAID 6 (Striping with Dual Parity)	**The Over-Protected Vault:** Similar to RAID 5, but two separate sets of parity information are distributed.	**Very high redundancy.** Can survive **two simultaneous drive failures**, which is important in large arrays.	**Highest cost** (loses two drives worth of capacity) and the **slowest write performance** of the common RAID types.	Large data archives and highly critical storage systems where data protection is paramount.