MODULE 7:
LEGAL GOVERNANCE, CYBER FORENSICS, CYBER INTELLIGENCE

Agencies in Australia that Investigate Cybercrime. Australia has established several key agencies dedicated to investigating cybercrime. These include the Australian Cyber Security Centre (ACSC), the Australian Federal Police (AFP), and the Australian Criminal Intelligence Commission (ACIC). These agencies work collaboratively to combat cyber threats, protect national interests, and maintain cybersecurity. Understanding their roles and cooperation is vital in the fight against cybercrime within the country.

Cyber forensics is a crucial discipline in the realm of cybersecurity. It involves the collection, preservation, analysis, and presentation of digital evidence to uncover cybercrimes. Cyber forensic experts use their skills to track down hackers, investigate data breaches, and support legal proceedings. This field plays a pivotal role in maintaining the security and integrity of digital information and is essential for both cybersecurity professionals and law enforcement agencies.

Cyber intelligence is the collection and analysis of data related to cyber threats and vulnerabilities. It provides insights into potential cyberattacks, helping organizations and governments take proactive measures to protect their information systems. In Australia, agencies like the Australian Signals Directorate (ASD) engage in cyber intelligence activities to safeguard national security. Cyber intelligence is a critical component of modern cybersecurity, enabling timely responses to emerging threats and ensuring the resilience of digital infrastructure. Understanding its principles is vital for cybersecurity professionals and policymakers alike.

7.1 AGENCIES THAT INVESTIGATE CYBER CRIME

The Commonwealth of Australia has a *National Plan to Combat Cybercrime* that includes a wide variety of agencies and stakeholders. The list that follows shows the spectrum of government agencies whose combined efforts amount to Australia's response to cybersecurity and cybercrime prevention.

- **Attorney-General's Department (AGD)**: formulates Commonwealth criminal law policy for parliament to enact. It includes such matters as personal identity security, privacy and wire-tapping policy.
- **Australian Criminal Intelligence Commission (ACIC)**: Australia's national criminal intelligence agency provides independent advice to government on current and developing risks of organised crime. ACIC has wide-ranging investigative capabilities from which it produces strategic intelligence assessments. It coordinates the effort to disrupt the impact of organised crime in Australia.

- **Australian Federal Police (AFP)**: Enforcement of federal criminal law and the proactive protection of Australia's interests from crime at home and overseas. The AFP has high capability to investigate, disrupt and apprehend cyber-criminals.
- **Australian Transaction Reports and Analysis Centre (AUSTRAC)** is the Australian government's financial intelligence agency that monitors financial transactions to detect money laundering, organised crime, tax evasion, welfare fraud and terrorism.
- **Commonwealth Director of Public Prosecutions (CDPP)**: Works with AFP and ACIC to prosecute offenders. Also provides advice to other prosecuting and investigating agencies at the State level in relation to cybercrime offences.
- **State and Territory law and justice agencies**: Concerned with criminal law policy at the state and Territory level.
- **State and Territory police**: Enforcement of State and Territory law. Police cybercrime units investigate all cyber offences against the person, business, and state, territory and local government.

Other related agencies:

- **CERT Australia**: The initial point of contact for cyber security incidents occurring in or impacting on Australian networks.
- **Australian Communications and Media Authority (ACMA)**: Notifies Internet Service Providers of transient threats such as malware identified among their customers. Also provides a channel of communication for reporting illegal online content.
- **Australian Competition and Consumer Commission (ACCC)**: Disrupts scams and prosecutes under the *Competition and Consumer Act 2010 (Cth)*.
- **Australian Security Intelligence Organisation (ASIO)**: Concerned with cyber activity for the purpose of espionage, sabotage, terrorism or other forms of politically motivated violence. Works with other investigatory agencies to prevent efforts directed against Australia.
- **Australia New Zealand Policing Advisory Agency (ANZPAA)**: A trans-Tasman advisory and coordinating body that provides policy advice on cross-jurisdictional issues.
- **CrimTrac**: A national database aimed at disseminating timely advice to state and federal agencies and stakeholders.
- **Department of Broadband, Communications and the Digital Economy (DBCDE)**: Responsible for the provision of internet services to government, industry and the community.
- **Department of Defence's Cyber Security Operations Centre (CSOC)**: Concerned with identifying sophisticated cyber threats against Australia.
- **Department of Foreign Affairs and Trade (DFAT)**: Protects Australia's interests by combating cybercrime internationally.
- **Department of the Prime Minister and Cabinet (PM&C)**: Central coordinator of cyber policy.

7.2 CYBER FORENSICS

Cyber forensics is an extensive discipline in its own right -- a fit topic for a course all its own. This section gives an overview of the discipline, highlighting methods and important considerations. While it will not make the average cyber-security professional a forensics expert, it will nonetheless acquaint them with the principles, and equip them to communicate with forensics consultants in a meaningful way.

LEGAL ISSUES

While a data breach cause might be determined through the application of forensic techniques, certain legal issues might complicate matters. For example, the *'Trojan Defence'* which allows an apparent perpetrator to argue that it was not they, but a piece of malicious computer code, or Trojan, that performed the actions unbeknown to them. A competent forensic investigator could anticipate this defence and obtain evidence to dismiss the argument.

SCENE OF THE CRIME

Information systems, as any cybersecurity professional will agree can be the 'scene of a crime' when a data breach has occurred. There will be evidence left behind of the perpetrators in the form network logs and other traces.

Organisations in recent years have employed forensics to investigate cases of:

- Hacking of commercially sensitive material
- Intellectual Property (IP) theft
- Fraud
- Forgery
- Bankruptcy
- Improper or illegal system use in the workplace
- Regulatory compliance

EVIDENCE MUST BE ADMISSIBLE IN COURT

Admissibility is a key consideration, and this means the evidence is accurate, not prejudicial and was legally obtained.

To ensure admissibility:

1. **Data** that may be subsequently relied upon in court **must not have been changed** during collection.
2. Persons with access to said data **must be competent** and have a legitimate reason for access.
3. **Access logs are kept** providing an audit trail of access, complete with details of who, what, where when and how access occurred, and any actions performed.

4. The **chief investigator has oversight** and is responsible for ensuring the law is always respected.

The forensic investigator will use a *"write-blocker"* to make an exact copy of an original hard disk, thus preserving the original in unchanged form.

INVESTIGATORY STAGES

Broadly speaking, the process can be divided into six stages:

1. **Readiness** – a proactive stance that ensures a system is in a state of functional readiness for forensic investigation. There are two aspects; the IT staff have been briefed and knows what needs to happen in the case of a breach, and secondly the investigator must be trained and competent.
2. **Evaluation** – in the event of an incident, it must be clear to all concerned what their role is and what the impact of the incident is likely to be.
3. **Collection** – the process of collecting evidence in a way that ensures admissibility in a court of law. This includes placing items in tamper-resistant bags and labelling them properly, conveying them to a secure environment as designated by law enforcement. Is also likely to involve interviewing various people.
4. **Analysis** -- must be accurate, thorough, impartial, recorded, repeatable and completed within the time-scales available and resources allocated.
5. **Presentation** – preparation of a report on findings written in plain language that non-forensic experts would understand. This would be in accordance with the initial instructions, plus any other relevant information.
6. **Review** – performed afterwards as a kind of lessons learned, process improvement exercise that identifies how the process might be done more efficiently in the future.

COUNTERMEASURES

Criminals engage in an on-going game of cat and mouse in which they constant seek loopholes in existing defences to exploit. Encryption is one such way; to prevent forensic analysis data may be over-written to render it unrecoverable. A files metadata can be changed, or the file subjected to "obfuscation" to disguise it.

7.3 DATA BREACH INTELLIGENCE

Data breach intelligence forms a subset of a larger threat intelligence landscape. There are categories of threat intelligence that agencies of all kinds (government and private) use to gather information that might be useful in proactively managing threat.

If you are a commercial organisation, or government department not directly concerned with legally sanctioned intelligence gathering, some of these methods will not be legally available.

INTELLIGENCE SOURCES

Cyber Security Intelligence analyses and disseminates tactical information about cyber threats, actors, and incidents. Cyber Security Intelligence can help organizations improve their cyber defence, response, and resilience.

Here are nine sources of Cyber Security Intelligence that can provide valuable insights and data:

PRIMARY SOURCES OF CYBER INTELLIGENCE

Cyber intelligence (CYBINT) is the collective name for data derived from a variety of intelligence-collection disciplines, as discussed below. CYBINT often gathers data from SIGINT (Signals intelligence), OSINT (Open-source intelligence) and ELINT (Electronic Intelligence). Less often it is derived from SOCMINT (Social Media Intelligence), HUMINT, GEOINT (discussed after this section).

1. **Signals intelligence** (SIGINT) derived from having listened into or intercepted the signals of persons of interest. In civil society, this is likely to be illegal, though in the defence of national interest, such methods are legally employed.
2. **Tech intelligence** (TECHINT) relates to information on the hardware and software capabilities of adversaries, allowing proper countermeasures.
3. **AlienVault Open Threat Exchange.** Categorised as Open-Source Intelligence (OSINT). This is one of the largest and most popular free open-source intelligence platforms, with over 100,000 participants sharing threat data and indicators of compromise (IOCs).
4. **ACSC Annual Cyber Threat Report**. Open-Source Intelligence (OSINT). This is an official report by the Australian Cyber Security Centre (ACSC), which provides an overview of key cyber threats impacting Australia, how the ACSC is responding to them, and crucial advice for Australian individuals and organisations to protect themselves online.
5. **CrowdStrike Global Threat Report**. Open-Source Intelligence (OSINT). This is an annual report by CrowdStrike, a leading cybersecurity company, that provides in-depth analysis of threat trends, adversary tactics, techniques, and procedures (TTPs), and recommendations for enhancing security posture.

6. **Threat Intelligence Communities.** Open-Source Intelligence (OSINT). Groups of individuals or organizations that share threat intelligence information and collaborate on cyber security issues. Threat intelligence communities can be formal or informal, public, or private, and have different levels of trust and access.
7. **Endpoint Devices**. These are the devices that connect to a network, such as computers, smartphones, tablets, and IoT devices. Endpoint devices can store useful data about user activity, system configuration, installed applications, and potential malware infections.
8. **Network Traffic**. This is the data that flows through a network, such as packets, protocols, ports, and IP addresses. Network traffic can reveal information about network topology, device communication, data exfiltration, and malicious activity.
9. **Threat Intelligence Platforms**. These are software tools that aggregate, correlate, and analyse threat data from multiple sources, such as feeds, reports, endpoints, and networks. Threat intelligence platforms can help automate threat detection, prioritization, and response.
10. **Threat Intelligence Providers**. Organizations that offer threat intelligence services or products to customers, such as reports, feeds, alerts, or analysis. Threat intelligence providers can have different areas of expertise, such as industry-specific threats, regional threats, or threat actor profiles.

SECONDARY SOURCES OF CYBER INTELLIGENCE

1. **Market intelligence** (MARKINT) helps in understanding the commercial environment of an adversary.
2. **Human intelligence** (HUMINT) through direct or indirect contact with people likely to have useful information. Might also be gathered through observation.
3. **Geospatial intelligence** (GEOINT) derived from sources such as GPS data and maps.
4. **Financial intelligence** (FININT) is information relating to the finances, or financial capabilities of adversaries. FININT is a principle tool in the fight against money laundering.

CREATE A CYBERTHREAT INTELLIGENCE PROGRAM (CIP)

As a complement to your Incident Response (IR) a Cyberthreat Intelligence Program (CIP) is an aspect of organisational risk management working in conjunction with the security operations centre (SOC) and producing information on request from management and board.

The CIP allows for the prioritization of attacks and the necessary updating of protective measures. It facilitates the early detection of incidents. It includes *operational* and *strategic* components. The operational component identifies and investigates incidents and fine-tunes the protection and detection processes. The

strategic component allows for networking with external parties who might be helpful, for example information sharing and analysis centres (ISACs) and other threat-sharing communities as well as specialist information providers. This networking allows for the identification of evolving threats, and of new and possibly disruptive technologies.

When setting up your CIP, the following points will be useful to consider.

- Identify from where you will be getting your data – this is a pre-requisite of properly defining the threat landscape.
- Concentrate your efforts on your specific business or sector because collecting intelligence that is not relevant will deplete your resources and divert attention.
- Create your table of priorities early and be disciplined in giving proper focus to the higher priorities, not allowing peripheral matters to deflect your efforts into less productive areas.
- Think of your CIP as a work-in-progress and deliberately build in the kind process improvement feedback loops that will allow the plan to evolve strategically over time.
- As far as possible automate the processing and dissemination of intelligence, as relying on manual processing is time consuming and limited in capability.

7.4 LEGAL ASPECTS OF CYBER RISK: STATE, NATIONAL & INTERNATIONAL

The ***International Legal Guide*** group based in London publish an excellent up-to-date country-by-country resource of the legal statutes applicable to cybersecurity at a state and national level.

The information available at their website is written in layperson's language but expressed with the precision that is the hallmark of legal writing. I would not attempt to summarise at the risk of misunderstanding and misrepresenting an issue in a small but significant way.

Follow the link below and peruse the entries to gain a view of the laws currently in force in relation to cybersecurity in Australia.

URL: https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/australia

It is segmented as follows:

1. **Cybercrime**
2. **Cybersecurity Laws**
3. **Preventing Attacks**
4. **Specific Sectors**
5. **Corporate Governance**
6. **Litigation**
7. **Insurance**
8. **Investigatory and Police Powers**

7.5 CASE STUDIES

Case Study 1: X, the sales manager of Company A gives 4 weeks' notice. Soon after he leaves, Company A receives advice from several clients that they received emails from an unknown Hotmail account containing defamatory information about Company A. Computer Forensics NZ Ltd (CFNZ) is instructed to search for evidence on X's PC that the emails originated from it.

During the briefing CFNZ suggests that the PC be examined for any evidence of any confidential data being copied to removable external media during the preceding 4 weeks.

Every bit and byte on the PC's hard disk is acquired and preserved using rigorous procedures as employed by NZ Police, the Serious Fraud Office, NZ Customs etc. The data is then meticulously analysed and various data (deleted) and system files are recovered showing that email data was created at the date and time that X was known to be operating the PC.

Detailed analysis also shows that during the last 3 days of X's employment 1 MYOB data file and 1 Microsoft Access file were copied to a USB drive. The files and detailed report are provided to Company A and appropriate discussions are held with the company's legal advisors for recommended action.

Case Study 2: Computer Forensics - Cyber CrimeIt was noticed by her manager that C's work output had been dropping over the previous 3 weeks, which coincided with the provision of broadband Internet to her department. It is visually established that she is spending many hours Internet 'surfing', which is specifically banned under her terms of employment.

She is cautioned appropriately but she continues with the unauthorised activity. Workmates also note that pornographic images are seen on her PC after the second caution.

The company subsequently dismisses her and within 14 days the company receives formal advice that it would be served with a charge of unjustified dismissal.

The manager convinces Management that all correct procedures were followed and that the Internet use was clearly beyond any amount or type that could be considered reasonable. Management decides to contest the action, especially as a significant amount of money is at risk and instructs CFNZ to analyse her PC for evidence of excessive Internet activity and deliberate entry to pornographic sites.

Analysis of her PC by CFNZ shows that incontestable evidence exists proving conclusively that the company's assertions were correct.

Finally, costs are awarded to the employer.