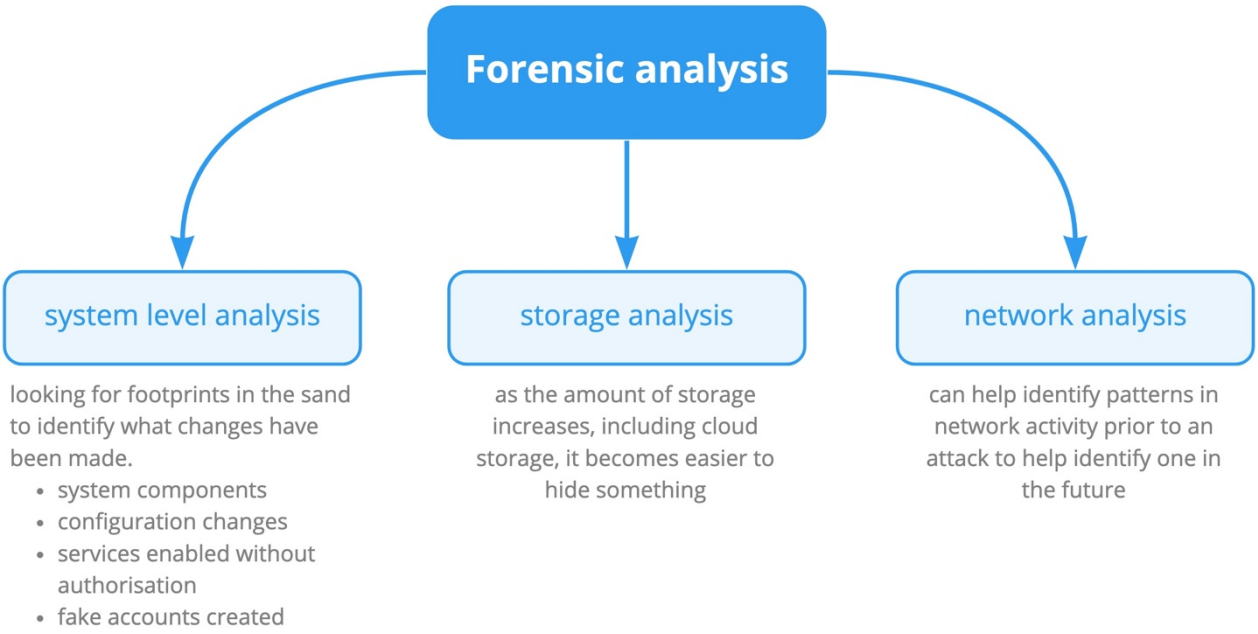
Chapter 10

Cyber security tools, techniques and reporting

Chapter learning objectives:

Lead	Component	Indicative syllabus content
D.3 Discuss cyber security tools and techniques.	Discuss: (a) Forensic analysis (b) Malware analysis (c) Penetration testing (d) Software security	• System level analysis, storage analysis and network analysis • Reverse engineering, decompilation and disassembly • Network discovery, vulnerability probing, exploiting vulnerabilities • Tiers of software security
D.4 Evaluate cyber risk reporting.	(a) Evaluate cyber risk reporting frameworks	• Description criteria including nature of business and operations, nature of information at risk, risk management programme objectives, cybersecurity risk governance structure etc.

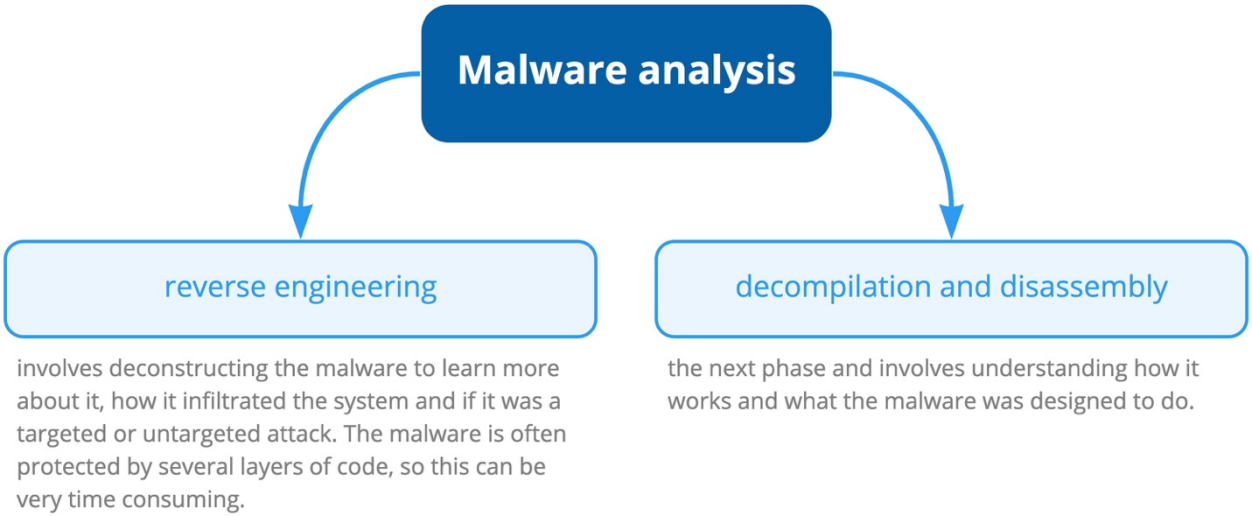
1. Forensic analysis



2. Malware analysis

The aim of malware analysis is to understand how the malware got into the computer and its purpose, including whether it was intended specifically for the organisation.

Obtaining this information means organisations are better able to improve their defences in the future.



3. Penetration testing

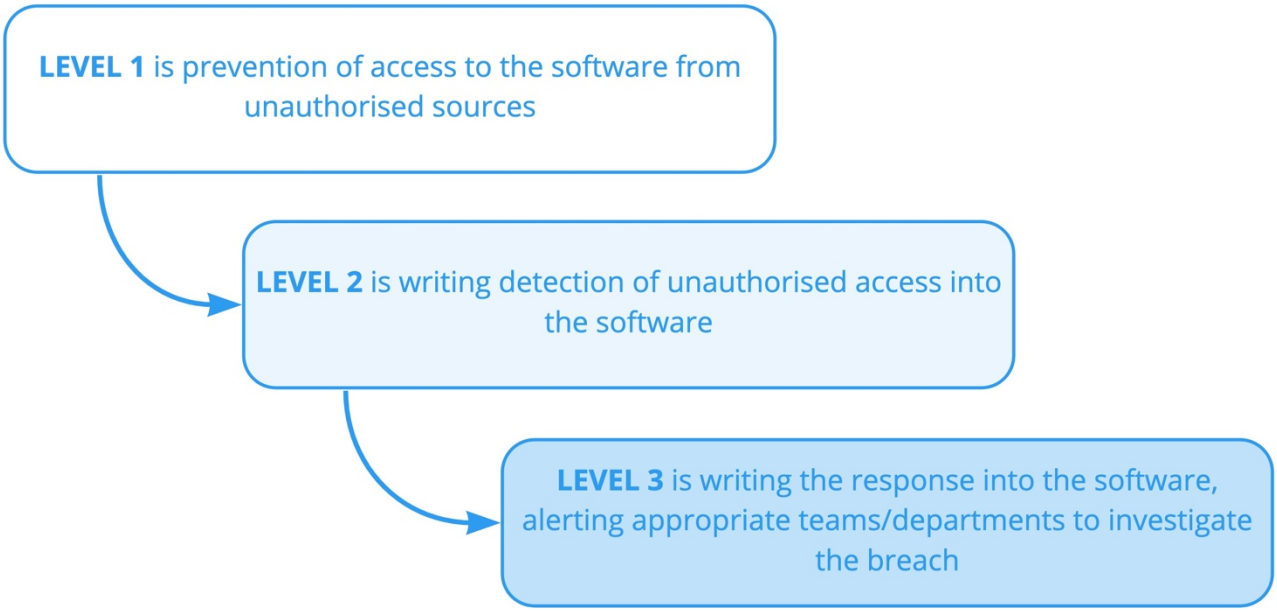
This is another aspect of prevention, where an organisation attempts to see how easily their systems can be breached, and often using white hat hackers.

Types of penetration testing

- **network discovery** this is about understanding the scope of a network, all of the devices that connect to a network from desktops and laptops, right through to smart phones and the internet of things.
- **vulnerability probing** identifying devices connected to the system that are the most susceptible to an attack.
- **exploiting vulnerabilities** where the white hat hacker attempts to gain access to the system, seeing how long it takes and what access can be gained.
- **internal network penetration testing** similar to the above, but the white hat hacker is granted an internal profile - it is important that organisations understand that there are not only external threats, but disgruntled employees could provide internal assistance to hackers.
- **web application penetration testing** looking for poor set up of web based applications (linked into application attacks from chapter 8), for example things like unprotected input boxes to enable SQL injection attacks.
- **wireless network penetration testing** this type of penetration testing seeks to identify any rogue devices on a network.
- **simulated phishing testing** where the organisation checks how well the workforce follow training/internal guidance with regards to phishing attempts.

4. Software security

Software security is important and has different levels.



Other considerations in software security

- **design review** is about considering the implications of technology development and the interconnectivity of devices - when software for some devices were designed previously, they did not have the structure that they have nowdays.
- **code review** considering how the code is written and how someone can prove that they are authorised to access to the software.
- **security testing** an internal audit type review to check controls are being carried out and are appropriate for the risk.

5. Digital resilience

Tucker Bailey, James Kaplan, Alan Marcus, Derek O'Halloran and Chris Rezek developed a concept called Digital Resilience - it involves 6 actions for an organisation to consider.

1) **Identify all the issues** - understand what an organisation has and how it is protected
2) **Aim toward a well-defined target** - set a stretching, understandable and achievable target. Including prioritisation of key issues and remembering basic controls - not just cyber security specifics.
3) **Work out how best to deliver the new cyber security system** - considering roles, responsibilities and potentially change the management structure.
4) **Establish the risk resource trade offs** - reviewing different potential solutions and selecting the most appropriate action to take.
5) **Develop a plan that aligns business and technology** - regulatory and future developments should be considered.
6) **Ensure sustained business engagement** - all employees must be involved and understand their role.

6. Frameworks

To assist organisations with their cyber security various groups and commentators have created some frameworks.

AICPA

- The AICPA is a global association formed by CIMA and the American Institute of Certified Public Accountants. AICPA stands for Association of International Certified Professional Accountants.
- In 2017 the AICPA launched a cybersecurity risk management reporting framework.
- The aim of the framework was to consider the needs of the various stakeholders in any organisation from the board, managers, investors, funding providers, etc by using a

common language for risk management reporting – along similar lines to financial reporting principles.

- Part of the process emphasises that cyber security is no longer just an IT problem (if it ever was just an IT problem) but it is part of the enterprise risk management process.

Cyber security risk management reporting

Management should prepare certain information:

- **Management's description** of the firm's cyber security activities.
- **Management's assertion** whether the risks were described in accordance with the criteria and whether appropriate controls were in place and effective.
- **The practitioner's opinion** of a qualified CPA on management's opinion.

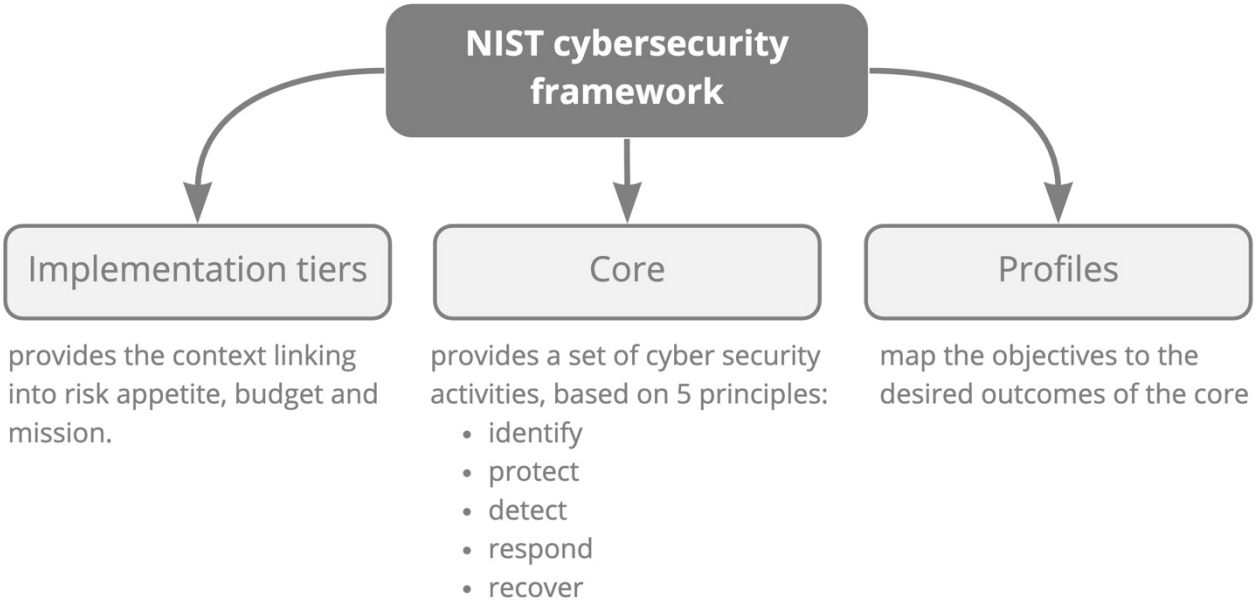
Criteria

- **Description criteria** – this is a very detailed document and links itself to the main content in chapters 8 and 9.
- **Control criteria** – this is a comprehensive document over 300 pages and lists out various potential risks and potential controls an organisation should have in place.

The result of this is the organisation's cybersecurity risk management report. There is an example of this report on the AICPA website.

NIST cybersecurity framework

The National Institutes of Standards and Technology (NIST - non-regulatory agency of the US department of Commerce) in the US provide the following framework as guidance. It involves 3 components:



AIC Triad

A commonly used framework, sometimes referred to as CIA Triad or the Security Triad.

It includes three elements:

- Availbility
- Integrity
- Confidentiality

ISO 270001

International Organisation for Standardisation (ISO) created a framework that focusses on all aspects of an organisation's information risk management processes.

The key principle behind the standard is to ensure a **proactive** rather than reactive approach to cyber security risk management:

- Define a security policy
- Define the scope of the Information Security Management System (ISMS)
- Conduct a risk assessment
- Manage identified risks
- Select control objectives and controls to be implemented
- Prepare a statement of applicability

7. Chapter summary