Chapter 3 summaries

Hacking definitions and nomenclature

- Hacking is thought to have existed since the late 1950s, but was originally used to describe legal activities such as the exploration of the potential of computers.
- Malicious hacking probably began in the early 1960s.
- Various terms have been introduced to try to distinguish between the criminal and non-criminal types of hacking, but most media sources and the general public still use the term 'hacking' to describe a criminal activity.
- Hackers can be differentiated by the use of the terms 'white-hat', 'black-hat' and 'grey-hat', depending on their ethical perspective and whether or not they cause malicious damage.
- Many companies employ 'ethical hackers' to test the security of their systems with their consent.
- Various sub-categories of hacker have been identified, including 'script-kiddies', 'cyberterrorists', 'wannabe lamers' and 'internals'.
- Labelling theory may have implications for hackers, as non-malicious hackers may feel that they are identified as criminals by others, and so may change their behaviour accordingly.

Types of hacking attack and known prevalence

- There are different types of hacking attack. These include:
    - Infiltration
    - Defacements
    - Denial of service (DoS) and distributed denial of service (DDoS).
- It is difficult to determine exactly how much hacking occurs, and it is expected that there is a high dark figure of hacking.

 Back to top

- The most recent figures from the Computer Security Institute indicate a drop in hacking levels.
- Statistics regarding non-corporate hacking victimisation are rare.

Methods of hackers

- Organisations such as the Honeynet project monitor the methods used by hackers so as to improve security.
- Hackers use many different methods to achieve their goals, but these can broadly be defined in terms of four categories.
    - Technical entry into the network
    - Social engineering
    - Dumpster diving
    - Physical entry.
- Not all these methods require the hacker to have advanced technical skills, but many hackers will use a variety of methods to achieve their goals.

Motives of hackers

- While a considerable amount has been written regarding the motives of hackers, much of this has been theoretical in nature, with relatively little empirical work.
- Many different motives for hacking have been proposed. Some of the most commonly proposed motives include peer-recognition, curiosity, need for power, alleviation of boredom, self-esteem and financial reasons.
- Attempts have been made to apply psychological theories, such as flow theory, the theory of planned behaviour and psycho-sexual theories, to hacking motives and behaviour.
- Not all studies have resulted in conclusive findings regarding the motives of hackers.

 Back to top

- In most cases, we are dependent on hackers to self-report their motives for hacking, which may result in biased information as they may be more inclined to respond in a socially acceptable manner.

Demographic characteristics of hackers

- The media stereotype suggests that hackers are mostly young males.
- While there are some exceptions, most research to date supports this stereotype.
- Hackers have also been found to have good educational levels.
- Other findings suggest that hackers are sometimes students or trainees, and can have above average income levels.

Ethical principles of hackers

- Various authors have suggested that most hackers subscribe either consciously or unconsciously to a code of ethics.
- The first such 'hacker ethic' was proposed by Levy (1984) and included principles such as:
    - Access to computers, and anything which might teach a person something about the way the world works, should be unlimited and total
    - All information should be free and available to the public, and secrecy should be avoided
    - Mistrust authority
    - Hackers should be judged by their hacking, and not by any other characteristic that they might exhibit or possess
    - The creation of art and beauty using computer technology is possible and should be encouraged

 Back to top

  - Computers can change one's life for the better.

- Several other authors have proposed more recent codes of ethics, including Mizrach and Tavani.

- While the hacker ethics generally appear positive, it is unclear exactly how many hackers truly subscribe to them, and even for those who do, there appear to be several loopholes within the principles.

Interpersonal relationships and other personality characteristics of hackers

- While some authors suggest that hackers have inferior interpersonal relationship skills, some empirical work indicates that hackers are capable of forming long-term relationships. However, these relationships may be slightly weaker than those of non-hackers.

- Hackers have also been found to be nocturnal in nature and task-oriented. There are conflicting findings regarding aggressiveness.

- Bachmann (2010) found that hackers preferred rational thinking styles over intuitive approaches, and they had higher risk propensity than the general public. These factors also influenced their success rates in hacking attempts.

Hacker groups versus lone hackers

- Some hackers prefer to work alone. One potential reason for this is an increased feeling of security. Lone hackers may form temporary alliances with other hackers as required.

- New hackers may seek out a more experienced hacker to act as a mentor. These hackers may later prefer a more solitary existence.

- Hacker groups may provide important psychological supports for members, particularly in terms of a sense of shared responsibility, feelings of belonging and personal identity development.

 Back to top

Punishment

- A variety of punishments have been used to penalise hackers, including fines, imprisonment, extradition and limiting access to computers.
- While hackers seem aware of the severity of potential punishments, this does not seem to act as much of a deterrent. This is possibly because hackers do not perceive punishment to be a likely outcome, and they perceive the benefits from hacking as outweighing the potential losses.

Prevention methods

- The prevention of hacking requires several approaches in order to be successful.
- Attempts can be made to identify young people who are at risk of becoming hackers, and intervention programmes can be developed.
- The availability of hacker tools can be restricted.
- Organisations and individual computer users can be educated about suitable methods to protect their systems, including both technological protection methods (such as firewalls) and reducing susceptibility to social engineering techniques.

 Back to top