Computer Law & Investigation

Corporate Investigation Part 1

Investigation

Criminal Investigation

- Hacking, Identity Theft, email bombing, Spam
- Sources of Law – Criminal Procedure Code, Evidence Act, Computer Misuse Act and Spam Control Act

Corporate Investigation

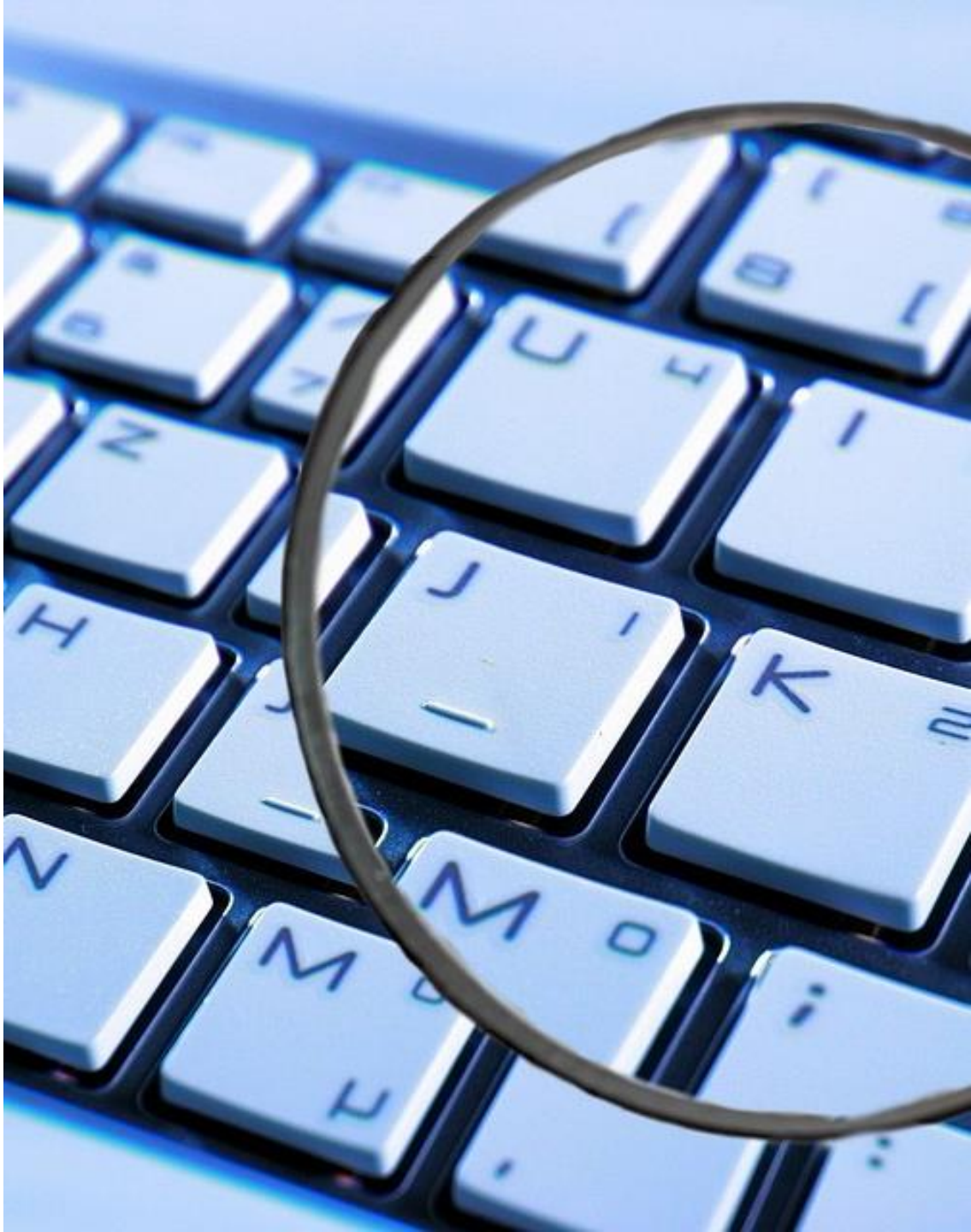
- Misuse of Co's resources, investigation into potential fraud
- Sources of "Law" – Computer User Policy Agreement, Corporate Security Policy, Privacy Laws, Data Protection Code, ISO 17799

Criminal Investigation

- Technology Crime Forensics Branch (TCFB), part of the Technology Crime Division of the Criminal Investigation Department (CID), one of the newest departments in the Singapore Police Force, has had its hands full since its inception in 1997.
- TCFB deals with the following:
  - Computer crimes such as the tampering of files and unauthorised access,
  - General offences in which technology is used in committing or abetting a crime, and
  - Technology-based commercial crimes such as online share frauds (eg; bogus investments, Pump & Dump)

Computer crime investigation using forensic tools

https://resources.infosecinstitute.com/computer-crime-investigation-using-forensic-tools-and-technology/?



Private Criminal Investigation

- Criminal Investigation and prosecution need not be done by the police alone.
- Victims of Criminal Activities can also proceed to prosecute cases themselves.
- Such cases normally refer to non-injury cases like
  - IT related offences like infringement of copyright and trademarks
  - Computer crimes
- Such cases would be prosecuted by private individuals often known as “Magistrate Complaints”.
- However, offences are usually those carrying only a fine or jail term less than 3 years

Private Criminal Investigation

- Section 12 Criminal Procedure Code
- Public Prosecutor may by fiat, and on such terms and conditions as he thinks fit, permit any person to prosecute, on the person's own behalf, any particular offence punishable under the Penal Code (Cap. 224) or any other written law, or to pursue any further proceedings in such prosecution.
- Commonly known as the Public Prosecutor's *fiat.*
- Usually for more serious offences that carry a jail term of more than 3 years

Corporate Investigation

- Commonly known as “non-criminal” investigation.
- Some commentators consider it “low-level investigations”.
- However, this does not mean less effort or less important than a criminal case.
- Computer Forensics is required usually in the following areas:
  - Commercial Fraud Cases like investigation of breaches of Directors Duties
  - Defamation cases like email investigation of libel and slander
  - Dishonesty among employees (using of company resources or sending spam using corporate accounts)

Sources of “Law”

- Does corporate personnel and his agents have the right to conduct forensics on another employee’s computer resources?
- The following documents are critical:
  - Computer User Policy Agreement / Corporate Security Policy,
  - ISO 17799,
  - Privacy Laws and Data Protection Code (Personal Data Protection Act)

User Policy Agreement (UPA)

- Most companies have UPA.
- UPA should be properly drafted so as to protect the company from liability and to allow the company to conduct investigations appropriately.
- However, most UPA are not well drafted to deal with the relevant scope to protect the interest of the company.

User Policy Agreement

Common UPA would include:

1. Define “Computer Resources”
   - “Computer resources” may be defined as human resources and all facilities and functions of a computer system – mainframe, distributed or workstation and all processing environments.
2. Prohibitions
   - Limited to organization-related work
   - No contravention of Copyright Act, Computer Misuse Act, Cybersecurity Act, Films Act, Penal Code, Undesirable Publications Act, Common Gaming Houses Act, Indecent Advertisements Act, Maintenance of Religious Harmony Act, PDPA etc.

User Policy Agreement

3. Powers to investigate & enforcement procedures
   - Use of covert surveillance
   - Search for information of all computer resources
   - Dispense with the right of privacy
4. Dispute Resolution
   - Who is the final arbitrator of disputes?
   - Sole decision of Chief Executive Officer, Chief Technology Officer, Member of the Board of Directors or mediators from Singapore Mediation Centre.
   - Decision shall be final and conclusive.

ISO 17799

https://www.iso.org/home.html

- ISO refers to “International Organisation for Standardisation”.
- “A comprehensive set of controls comprising best practices in information security”
- Comprises TWO parts - a code of practice (ISO17799) and a specification for an information security management system (BS7799-2)
- Basically… an internationally recognised generic information security standard
- Singapore Standards Council is a member of ISO

https://www.youtube.com/watch?v=AYBVTeqKahk&feature=youtu.be

Objectives

- “It is intended to serve as a single reference point for identifying a range of controls needed for most situations where information systems are used in industry and commerce”
- Essentially the facilitation of trading in a trusted environment
- Established as THE major standard for information security
- When creating a new policies/etc ensure they covers all ISO 17799 issues

Contents of ISO 17799

1. Business Continuity Planning
To counteract interruptions to business activities and to critical business processes from the effects of major failures or disasters.

2. System Access Control
To control access to information and to prevent unauthorised access to information systems.

Contents of ISO 17799

3. System Development and Maintenance
To prevent loss, modification or misuse of user data in application systems and to protect the confidentiality, authenticity and integrity of information;

4. Physical and Environmental Security
To prevent unauthorised access, damage and interference to business premises and information; to prevent loss, damage or compromise of assets and interruption to business activities; to prevent compromise or theft of information and information processing facilities.

Contents of ISO 17799

5. Compliance
To avoid breaches of any criminal or civil law, statutory, regulatory or contractual obligations and of any security requirements and to ensure compliance of systems with organizational security policies and standards

6. Personnel Security
To reduce risks of human error, theft, fraud or misuse of facilities; to ensure that users are aware of information security threats and concerns, and are equipped to support the corporate security policy in the course of their normal work; to minimise the damage from security incidents and malfunctions and learn from such incidents.

Contents of ISO 17799

7. Security Organisation
To manage information security within the Company;

To maintain the security of information when the responsibility for information processing has been outsourced to another organization.

8. Computer & Network Management
To minimise the risk of systems failures and to protect the integrity of software and information

Contents of ISO 17799

9. Asset Classification and Control

The objectives of this section are: To maintain appropriate protection of corporate assets and to ensure that information assets receive an appropriate level of protection.

10. Security Policy

The objectives of this section are: To provide management direction and support for information security.

Balancing Security and Privacy

- Many unresolved issues/problems.
- Privacy Law in Singapore?
  - Personal Data Protection Act
  - Law of Confidential Information
- Is it right to tilt the balance against privacy in the interest of security?

End of Lecture