InfoSec Tutorial: Legal, Ethical and Forensic Issues

Tony Kenyon, CEO.

Revision 1.01.

Updated: Jan 5th 2006

Ref: CNXT0001

Law Investigation & Ethics

- Ethics covered by several standards bodies, including:
  - ISC^2, IAB, Computer Ethics Institute (CEI)
- Crimes
  - Two main categories: with computer, against computer systems
  - Main Types are:
    - DOS. Network Intrusion. Maliscious code. Use of readily avilable Attack scripts
    - Password theft. Emanation eavesdropping
    - Social engineering
    - Illegal content. Software piracy
    - Fraud. Enbezzlement
    - Spoofing of IP addresses. Masquerading
    - Dumpster diving. Espionage. Information warfare. Terrorism
    - Destruction or alteration of information. Data-diddling

Law Investigation & Ethics

- Different legal systems: Common Law, Islamic & other religious Law, Civil Law.
  - Common Law adopted by US, UK, Canada, Australia
  - Civil Law adopted by France, Germany, Quebec etc.
- US
  - Statutory Law
  - Administrative Law
  - Common Law

US Statutory Law

- E.g. 18 USC 1001 (1992) (sec 1001 of Title 18 ”Crimes and Criminal Procedures”)
  - Title 18 used for many computer crime prosecutions
  - 18 USC 1030 (1986) covers Computer Fraud and Abuse Act.
- Others:
  - Title 12 banks and Banking
  - Title 15 Commerce and Trade.
  - Title 26 Internal Revenue Code
  - Title 49 Transportation.

US Administrative Law

- CFR (code of Federal Regs)

US Common Law

- Three Main Types
  - Criminal Law.
  - Civil Law.
  - Adminstrative/Regulatory Law.
  - Only Civil Law cannot carry imprisonment.
- And..
  - Intellectual Property Law
    - Patent, Copyright. Trade Secrets. Trademark.
  - Information Privacy Law
    - EU laws more protective of invividual privacy than the US.

Legal Issues – Data Protection

- Heathcare
  - Information cannot b reused for another purpose
  - Information must be availble to the source and can be corrected by the source

Legal Issues - Email Monitoring

- Monitoring
  - All users must be informed that monitoring is taking place by using a frequent notification or prominant login banner
  - Message should state that punishment is possible and compliance indicates consent. System should NOT guarantee email privacy.
  - Monitoring must be uniformly applied across all employees.
  - Explain acceptable use, who can read email, and how long it is backed up.

Legal Issues – Web Access

- P3P (Platform for Privacy Preferences)
  - Developed by WWWC (W3C) for privacy practices on Web Sites.
  - Standard is P3P 1.0 Jan 28 2002 (www.w3.org/TR)
  - Who has access to info, type of info collected, how info is used, legal entity making the statement.
  - Supports user agents for browser configuration for comparison with web servers
  - Has serious limitations in protction of privacy though.
- EPIC (www.epic.org)
  - Critical of P3P because it forces users to accept privacy levels lower than **US Code of Fair Practices**, for web access. Also because P3P is perceived to be complex, may cause users to bypass annoyance messages, and some W3C members are businesses (potential conflict).
- See **Fair Information Practice Principles**.

Legal Issues – Forensics

- Many difficulties in investigating and prosecting computer criminals
- Evidence Gathering, Storage and Preservation are critical in legal procedings
- MOM (Motive Opportunity Means) to conduct a crime
- US FBI and Secret Services have juristiction over computer crime
  - In US senior corporate officers can be liable up to $290m
  - May need a warrant unless imiment danger of information being damaged or lost.
  - Legal Liability determined if Cost of Control < Potenial Loss

Legal Issues

- Encryption export Issues
  - US relaxed export restrictions in July 2000 to certain countries
  - ANY encryption product can be shipped to ANY user
  - Covered EU and 8 other trading partners
- Pace of technology means that ”Embezzlement, Fraud and Wiretapping” law is used to prosecute compuetr crime
- Computer evidence is generally considered ’Hearsay’, and mostly intangible

Legal Issues – Evidence

- Evidence Gathering, Storage and Preservation are critical in legal procedings
- Chain of Evidence
  - Location obtained
  - Time obtained
  - Who discovered the evidence
  - Who secured the evidence
  - Who controlled the evidence and/or maintained possession of it
- Evidence Lifecycle
  - Discovery -> Return to owner

Legal Issues – Evidence

- To be admissable in a court of Law evidence must be:
  - Relevant
  - Legally Permissable
  - Reliable
  - Properly Identified
  - Properly Preserved
- Types of Evidence
  - Best (original)
  - Secondary (copy)
  - Direct (proves/dosproves act through testimony by witness)
  - Conclusive (incontravertible)
  - Opinion (expert, non-expert)
  - Circumstantial
  - Hearsay

Computer Evidence

- Classified as Hearsay by default
- Viewed as Intangible

Legal Issues - Ethics

- ISC^2 Code of Ethics
- Computer Ethics Institute
- Internet Activities Board (IAB) Ethics & the Internet RFC 1087
- US Dept of Health, Education & Welfare Code of Fair Information Practices
- Organisation for Economic Cooperation & Development (OECD)

Intellectual Property

- Patents
- Trade marks
- Service Marks
- Copyright
- etc

Further Research

- Key standards with annotated purpose
- Standards of Ethics
- Due Care, Prudent Man, Pen Register,
- ESIGN, HIPPA, PATRIOT ACT, EU CAD
- Escrow, Carnivore (ISP), Eschelon.
- Chain of Evidence verses Evidence Lifecycle.
- Expert witness, evidence admissability.

Questions?