Legal, Regulations, Compliance and Investigations

Mike Smith

26/04/10 - Rev.25

Due ...

- **Diligence** - Do **Detect** - Steps to identify risks using best practices - investigated weaknesses
- **Care** - Do **Correct** - Steps taken to correct identified risks to a minimum - did all it could to prevent security breaches with proper controls and countermeasures

Evidence

- Best - primary, original, not oral
- Secondary - copies of documents and oral evidence
- Direct - does not need backup - witness account
- Conclusive - irrefutable
- Circumstantial - prove an intermediate fact
- Corroborative - supplementary
- Opinion - only the facts not opinions
- Hearsay - oral or written too far removed

Incident Response

Steps

1. Triage
2. Investigation
3. Containment
4. Analysis
5. Tracking
6. Recovery

Develop a Team

- Various BUs
- Virtual
- Permanent
- Hybrid
- CERT Mailing List
- CERT Documents

- Management decide on calling Cops

Computer Forensics

- International Organization on Computer Evidence - IOCE
- Scientific Working Group on Digital Evidence - SWDGE
- MOM - Motive, Opportunity and Means
- Locard's Principle of Exchange
- Identification - Preservation - Collection - Examination - Analysis - Presentation - Decision
- Primary / Working Image - First thing make a bit mirror copy
- Chain of Custody - Evidence labeled indicating who secured and validated it

Cybercrime

- Computer-assisted
- Computer-targeted
- Computer is incidental

OECD 7 Principles

- Collection should be limited and lawful
- Personal data should be complete and current
- Subjects should be notified of the reason for collection
- Disclosure only with consent
- Reasonable safeguards in place
- Practices and policies openly communicated
- Subjects should be able to find and correct personal info
- Organizations should be accountable

Types of Law

- Civil (Code) Law - continental Europe
- Common Law - England
  - Criminal - jail
  - Civil/tort - damages
- Customary Law
- Religious Law Systems
- Mixed Law Systems

Intellectual Property Law

- Trade Secret - important for company survival
- Copyright - protects the expression of the idea of the resource not the resource itself e.g. computer programs and manuals
- Trademark - word, name, symbol, sound, shape
- Patent - novel invention

Software

- Freeware
- Shareware or trialware
- Commercial
- Academic

Dealing with Privacy

- Government Regs - SOX, HIPPA, GLBA, BASEL
- Self-regulation - Payment Card Industry - PCI
- Individual user - Passwords, encryption, awareness