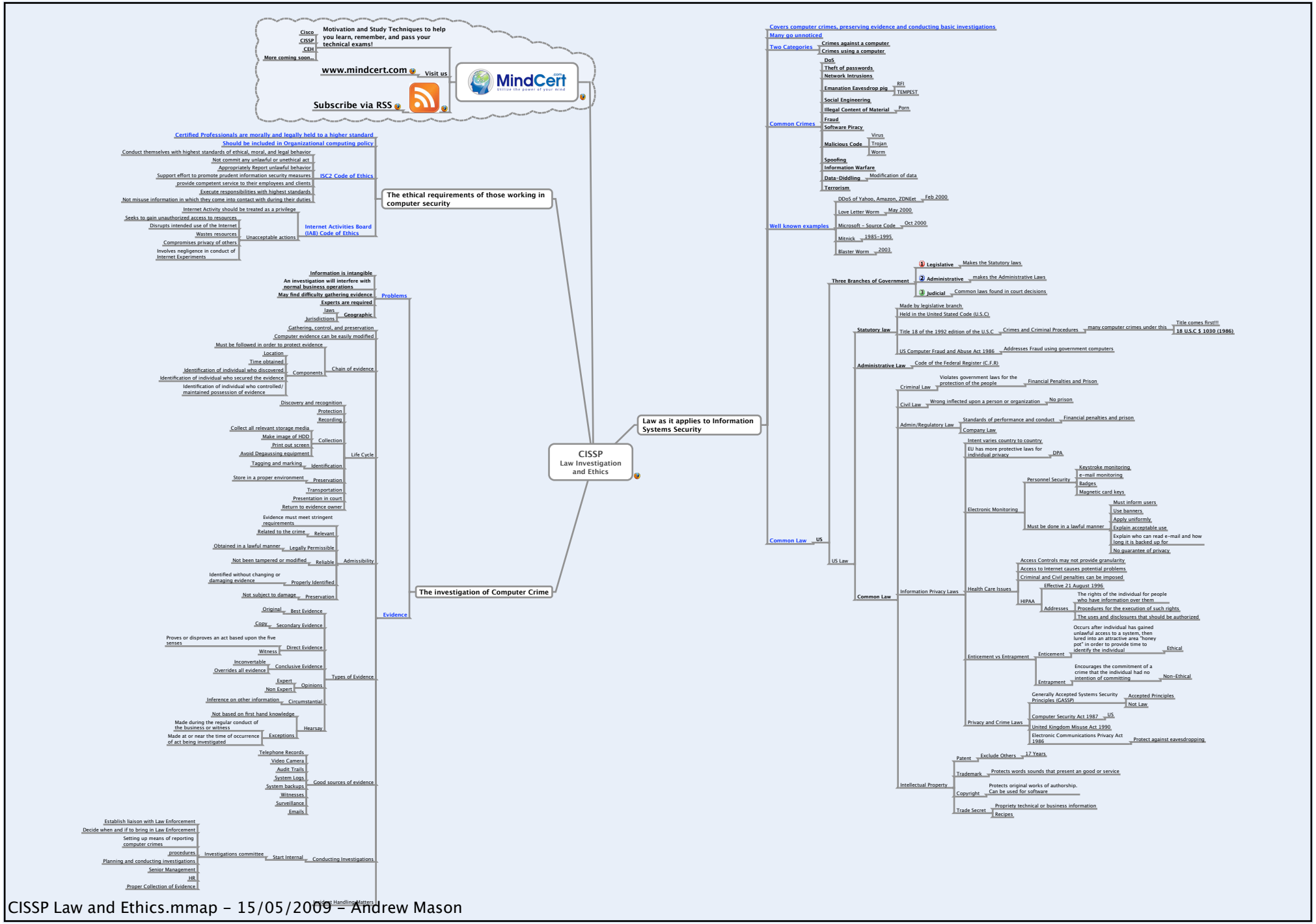
Motivation and Study Techniques to help you learn, remember, and pass your technical exams!
Cisco
CISSP
CEH
More coming soon...
www.mindcert.com
Visit us
Subscribe via RSS
MindCert.com
utilize the power of your mind
CISSP
Law Investigation and Ethics
The ethical requirements of those working in computer security
Certified Professionals are morally and legally held to a higher standard
Should be included in Organizational computing policy
ISC2 Code of Ethics
Conduct themselves with highest standards of ethical, moral, and legal behavior
Not commit any unlawful or unethical act
Appropriately Report unlawful behavior
Support effort to promote prudent information security measures
provide competent service to their employees and clients
Execute responsibilities with highest standards
Not misuse information in which they come into contact with during their duties
Internet Activities Board (IAB) Code of Ethics
Internet Activity should be treated as a privilege
Unacceptable actions
Seeks to gain unauthorized access to resources
Disrupts intended use of the Internet
Wastes resources
Compromises privacy of others
Involves negligence in conduct of Internet Experiments
The investigation of Computer Crime
Problems
Information is intangible
An investigation will interfere with normal business operations
May find difficulty gathering evidence
Experts are required
Jurisdictions
Geographic laws
Evidence
Chain of evidence
Gathering, control, and preservation
Computer evidence can be easily modified
Must be followed in order to protect evidence
Components
Location
Time obtained
Identification of individual who discovered
Identification of individual who secured the evidence
Identification of individual who controlled/ maintained possession of evidence
Life Cycle
Discovery and recognition
Protection
Recording
Collection
Collect all relevant storage media
Make image of HDD
Print out screen
Avoid Degaussing equipment
Identification
Tagging and marking
Preservation
Store in a proper environment
Transportation
Presentation in court
Return to evidence owner
Admissibility
Evidence must meet stringent requirements
Relevant
Related to the crime
Legally Permissible
Obtained in a lawful manner
Reliable
Not been tampered or modified
Properly Identified
Identified without changing or damaging evidence
Preservation
Not subject to damage
Types of Evidence
Best Evidence
Original
Secondary Evidence
Copy
Direct Evidence
Proves or disproves an act based upon the five senses
Witness
Conclusive Evidence
Inconvertable
Overrides all evidence
Opinions
Expert
Non Expert
Circumstantial
Inference on other information
Hearsay
Not based on first hand knowledge
Exceptions
Made during the regular conduct of the business or witness
Made at or near the time of occurrence of act being investigated
Good sources of evidence
Telephone Records
Video Camera
Audit Trails
System Logs
System backups
Witnesses
Surveillance
Emails
Conducting Investigations
Establish liaison with Law Enforcement
Decide when and if to bring in Law Enforcement
Setting up means of reporting computer crimes
Start Internal
Investigations committee
procedures
Planning and conducting investigations
Senior Management
HR
Proper Collection of Evidence
Incident Handling Matters
Law as it applies to Information Systems Security
Covers computer crimes, preserving evidence and conducting basic investigations
Many go unnoticed
Two Categories
Crimes against a computer
Crimes using a computer
Common Crimes
DoS
Theft of passwords
Network intrusions
Emanation Eavesdrop pig
RFI
TEMPEST
Social Engineering
Illegal Content of Material
Porn
Fraud
Software Piracy
Malicious Code
Virus
Trojan
Worm
Spoofing
Information Warfare
Data-Diddling
Modification of data
Terrorism
Well known examples
DDoS of Yahoo, Amazon, ZDNEet
Feb 2000
Love Letter Worm
May 2000
Microsoft - Source Code
Oct 2000
Mitnick
1985-1995
Blaster Worm
2003
US Law
Common Law
US
Three Branches of Government
1 Legislative
Makes the Statutory laws
2 Administrative
makes the Administrative Laws
3 Judicial
Common laws found in court decisions
Statutory law
Made by legislative branch
Held in the United Stated Code (U.S.C)
Title 18 of the 1992 edition of the U.S.C
Crimes and Criminal Procedures
many computer crimes under this
Title comes first!!!
18 U.S.C § 1030 (1986)
US Computer Fraud and Abuse Act 1986
Addresses Fraud using government computers
Administrative Law
Code of the Federal Register (C.F.R)
Criminal Law
Violates government laws for the protection of the people
Financial Penalties and Prison
Civil Law
Wrong inflicted upon a person or organization
No prison
Admin/Regulatory Law
Standards of performance and conduct
Financial penalties and prison
Company Law
Common Law
Information Privacy Laws
Intent varies country to country
EU has more protective laws for individual privacy
DPA
Health Care Issues
Personnel Security
Keystroke monitoring
e-mail monitoring
Badges
Magnetic card keys
Electronic Monitoring
Must be done in a lawful manner
Must inform users
Use banners
Apply uniformly
Explain acceptable use
Explain who can read e-mail and how long it is backed up for
No guarantee of privacy
Access Controls may not provide granularity
Access to Internet causes potential problems
Criminal and Civil penalties can be imposed
HIPAA
Effective 21 August 1996
Addresses
The rights of the individual for people who have information over them
Procedures for the execution of such rights
The uses and disclosures that should be authorized
Enticement vs Entrapment
Enticement
Occurs after individual has gained unlawful access to a system, then lured into an attractive area "honey pot" in order to provide time to identify the individual
Ethical
Entrapment
Encourages the commitment of a crime that the individual had no intention of committing
Non-Ethical
Privacy and Crime Laws
Generally Accepted Systems Security Principles (GASSP)
Accepted Principles
Not Law
Computer Security Act 1987
US
United Kingdom Misuse Act 1990
Electronic Communications Privacy Act 1986
Protect against eavesdropping
Intellectual Property
Patent
Exclude Others
17 Years
Trademark
Protects words sounds that present an good or service
Copyright
Protects original works of authorship.
Can be used for software
Trade Secret
Propriety technical or business information
Recipes