CISSP Final Day Review

I. Security Management Practices

- A. Responsibility of security more on individual now in a distributed environment.
- B. Security through obscurity
- C. Data owners, data custodians, users
  - 1. Data owner responsible for classification and level of security required.
- D. Administrative controls
  - 1. Policies, employee education, change control, employee management, data classification
- E. Control should be visible for deterrence, but internal mechanisms hidden
- F. Due care
- G. CIA triad
  - 1. Confidentiality, integrity, availability
- H. Shoulder surfing – confidentiality
- I. Social engineering – confidentiality
- J. DoS – availability
- K. Open system = built to standards
- L. Closed system = proprietary
- M. Vulnerability, threat, risk, exposure, countermeasure
- N. Assurance = sum total of all security components providing a level of confidence
- O. Risk management and analysis
  - 1. Identify assets and assign values
  - 2. Identify risks
  - 3. Quantify impact of risks
  - 4. Provide economical countermeasures
  - 5. Cost/benefit for each countermeasure
    - a. ALE before and after countermeasure and annualized cost of countermeasure
  - 6. Team members from different departments
  - 7. Delayed versus potential losses
  - 8. Qualitative versus Quantitative
    - a. Delphi method = anonymously giving opinion – qualitative approach
  - 9. Asset value x exposure = single loss expectancy
  - 10. SLE x annualized rate of occurrence = annualized loss expectancy
  - 11. Total risk = before countermeasure
  - 12. Residual risk = after countermeasure
  - 13. Transfer, reduce, accept, reject risk

- P. Security program
  - 1. Management support number 1 issue
  - 2. Issue specific versus organizational policies
  - 3. Department versus enterprise wide policies
  - 4. British Standard 7799
  - 5. Standards, Baselines, Guidelines, Procedures
  - 6. Top-down versus Bottom-up approaches
  - 7. Data classification
    - a. Data owner responsibility
  - 8. Employee management
    - a. Firing, hiring, non-disclosure
      - i. Non-friendly = disable account and change passwords
    - b. Separation of duties
      - i. Collusion

II. Access Control

- A. Subject, object, access (flow of information between the two)
- B. Identification, authentication, authorization
- C. Prove identity with something you know, have, are
- D. Strong authentication – 2 factor
- E. Passwords, cheapest, lowest security – biometrics, most expensive, highest security
- F. Biometrics
  - 1. Type I (reject authorized) Type II (accept imposter)
  - 2. CER (Crossover Error Rate) is when Type I = Type II
- G. Retina scan
  - 1. Blood vessel pattern in back of eye
- H. Iris scan
  - 1. Coloration around pupil
- I. Hand geometry
  - 1. Width of hand and fingers – form of hand
- J. Hand topology
  - 1. Side view of hand
- K. Signature dynamics
  - 1. Process of someone writing his or her name
- L. Password generator = users may write down complex passwords
- M. Dictionary and brute force attack
- N. Cognitive password = fact or opinion-based
- O. One-time passwords
  - 1. Token device
    - a. Synchronous – time or event based
    - b. Asynchronous – challenge response
- P. Replay attacks = reusing credentials
  - 1. Time stamps, one time passwords, digital signatures are countermeasures

Q. Passphrase turned into virtual password

R. Memory and smart cards
   1. Smart = can process data

S. Single Sign-on
   1. Kerberos, SESAME, Scripts, thin clients
   2. Secure European System for Applications in a Multi-vender Environment – public key cryptography and PACs
   3. Kerberos, principals, KDC, AS, TGS, realm, secret and session key
      a. Symmetric keys
      b. Tickets similar to certificates in PKI

T. Access control models
   1. DAC
      a. Data owner
      b. Access control matrix
   2. RBAC
      a. Mapping to role in organization – based on tasks
   3. MAC
      a. Security labels, clearance, classification, categories (need to know)

U. Restrict interface
   1. Menus, shells, database views, physical constrained

V. Access Matrix
   1. ACL column – bound to device
   2. Capability row – bound to user

W. Centralized (RADIUS, TACACS, Diameter)

X. Decentralized

Y. Auditing is a technical control

Z. Log protection
   1. Hashing, permissions, digital signatures

AA. Unauthorized disclosure of info
   1. Social engineering, object reuse, electrical signals
   2. Signal capturing
      a. TEMPEST, control room, white noise

BB. Honey pot
   1. Enticement and entrapment

CC. Padded cell
   1. Virtual environment

DD. Denial of service

EE. Spoofing

FF. Man in the middle

GG. Spamming and mail relay

HH. War dialing
   1. Program dials a bank of phone numbers

III. Business Continuity Planning (BCP) and Disaster Recovery Planning (DRP)

- A. DRP = procedures for during and right after a disaster or disruption
  - 1. Emergency response
- B. BCP = procedures to keep business running after disaster or disruption
- C. Both plans should be integrated into business decisions and made part of the security program
- D. Business Impact Analysis (BIA)
  - 1. First step in developing BCP and DRP
  - 2. Identify critical and the duration the company can handle being without them, vulnerability analysis, quantify impact of threats, identify viable alternatives
- E. Enterprise and departmental plans
- F. Reciprocal agreements
  - 1. Not enforceable
- G. Alternative sites
  - 1. Hot = expensive, fully equipped, ready in hours
  - 2. Warm = less expensive, peripheral devices
  - 3. Cold = least expensive, environmental controls only, hard to test
- H. Disk shadowing
  - 1. Mirroring
- I. Electronic vaulting (off site)
  - 1. Transfer bulk backup info
- J. Remote journaling
  - 1. Transfer transaction logs and changes, not full file
- K. Emergency state is over when company returns to primary site
- L. Least critical department moved back to primary site first
- M. Testing and drills
  - 1. Checklist Test
    - a. Copies of plan distributed to different departments
  - 2. Structured Walk-Through Test
    - a. Representations from each department go over the plan
  - 3. Simulation Test
    - a. Going through a disaster scenario
    - b. Continues up to the actual relocation to an off-site facility
  - 4. Parallel Test
    - a. Systems moved to alternate site and processing takes place there
  - 5. Full-Interruption Test
    - a. All of processing moved to off-site facility

IV. Cryptography

- A. Substitution and transposition ciphers
  - 1. Caesar cipher is a simple substitution cipher
- B. Non-repudiation
  - 1. Cannot deny sending

C. Cryptanalysis
  1. Breaking encryption

D. Key clustering
  1. Two different keys generate the same ciphertext from the same plaintext

E. Key and keyspace
  1. Larger keyspace allows for more keys. Full space should be used

F. Work factor
  1. Amount of work to break encryption

G. Frequency analysis attack
  1. Identify patterns

H. Running key and concealment ciphers

I. Steganography
  1. Hiding the existence of data

J. Clipper Chip
  1. Hardware chip
  2. Skipjack algorithm, 80-bit key, possible backdoor

K. Fair Cryptosystems
  1. Software, public-key cryptography

L. Block and stream ciphers
  1. Block = software
  2. Stream = hardware

M. Symmetric
  1. Faster than asymmetric ✓
  2. Out-of-band key exchange
  3. Examples
     a. Data Encryption Standard (DES)
     b. Blowfish
     c. Twofish
     d. IDEA
     e. RC4, RC5, RC6

N(N-1)/2 40 keys [illegible]

RC#

R I D
S D E
A E S
A

N. Asymmetric
  1. Encrypt symmetric key ✓
  2. Examples
     a. RSA
     b. Elliptic Curve Cryptosystem (ECC)
     c. Diffie-Hellman
     d. El Gamal
     e. Knapsack

R
E
D
E
K

O. RSA
  1. Security from difficulty of factoring large number into 2 prime numbers
  2. Trapdoor = knowing the secret to factor to prime numbers

P. Diffie-Hellman, DSA, El Gamal
  1. Discrete logarithms in a finite field

Q. Session key

   1. Symmetric key, good for only one session

R. Data Encryption Standard
   1. 56-bit true key, block symmetric cipher
   2. Lucifer
   3. 64-bit blocks go through 16 rounds of transposition and substitution
   4. Data Encryption Algorithm

S. Electronic Code Book (ECB)
   1. Patterns – least secure

T. Cipher Block Chaining (CBC)
   1. Most commonly used – using ciphertext from last block

U. Cipher Feedback (CFB), Output Feedback (OFB) modes
   1. Simulates stream cipher

V. Advanced Encryption Standard
   1. Rijndael
   2. Block symmetric cipher
   3. Key sizes = 128, 192, 256

W. Trapdoor one-way function
   1. Security of RSA asymmetric algorithm

X. Zero-proof knowledge
   1. Telling something without telling the whole story
   2. Using cryptographic key without showing it

Y. PKI
   1. Certificates
      a. Contains public key
      b. Binds individual to certificate
   2. CA
      a. Validates and vouches for owner of certificate
   3. Certificate Revocation List
      a. List of certificates that have been revoked
   4. Registration Authority
      a. Cannot issue certificates

Z. Hashes
   1. SHA = 160-bit digest
   2. HAVAL = variable length digest
   3. MDs = 128-bit digest

AA. Birthday attack
   1. Hashing algorithms with longer message digest not as vulnerable

BB. Message authentication code (MAC)
   1. Hash algorithm + symmetric key Integrity √'d by other party

CC. Digital signature (AIN)
   1. Encrypt message digest with private key
   2. Authenticity and integrity and non-repudiation

DD. Digital Signature Standard (DSS)
   1. DSA, SHA, ECDSA, RSA
      a. DSA cannot encrypt data or exchange keys

EE. One-time pad

1. Most secure encryption mechanism
2. Pad is at least as large as the message

FF. Link encryption and end-to-end encryption
  1. Header has to be decrypted at each hop for link encryption

GG. Privacy-Enhanced Mail (PEM)
  1. Secure e-mail standard

HH. Message Security Protocol (MSP)
  1. Military's PEM

II. Pretty Good Privacy
  1. Web of trust, peer trust relationship
  2. Phil Zimmermann

JJ. SHTTP = encrypt message

KK. HTTPS = encrypts channel

LL. Secure Electronic Transaction (SET)
  1. E-commerce, Visa and MasterCard
  2. PKI

MM. SSH
  1. Works like a tunneling protocol
  2. Terminal session – use instead of Telnet or r-utilities

NN. S/MIME
  1. Secure Multipurpose Internet Mail Extensions
  2. Extending functionality of MIME and provides security

OO. SSL
  1. Uses public key cryptography
  2. Secure channel

PP. IPSec (Ai V)
  1. Transport mode
    a. Protect payload
  2. Tunnel mode
    a. Protect payload and headers
  3. Authentication Header (AH) protocol
    a. Integrity Check Value (ICV) – system authentication and integrity
    b. Sequence numbers to protect against replay attacks
  4. Encapsulating Security Payload (ESP)
    a. Same functionality as AH, but also provides encryption
  5. Security Association (SA)
    a. Agreed upon parameters
    b. One for each direction
  6. Security Parameter Index (SPI)
    a. Indicates what SA to use
  7. Internet Key Exchange (IKE)
    a. Hybrid of Internet Security Association and Key Management Protocol (ISAKMP) and Oakley key exchange
      i. ISAKMP = framework (Network layer) SKIP (Network layer)
      ii. Oakley = does negotiation of session

QQ. Active attack = doing something versus passive attack = sniffing or eavesdropping

RR. Ciphertext-only attack
   1. Have ciphertext

SS. Known-plaintext attack
   1. Have ciphertext and plaintext

TT. Chosen-plaintext attack
   1. Can choose what plain text gets encrypted

UU. Chosen-ciphertext attack
   1. Can choose what cipher text gets decrypted

VV. Man-in-the-middle attack
   1. Insert self into active session

WW. Kerchoff's Principle
   1. Algorithm known and key is secret

V. Telecommunications and Network Security

A. TCP/IP = protocol suite of the Internet

B. Socket = address plus port

C. TCP = connection-oriented
   1. Reliable, congestion control, more overhead, sequence numbers

D. UDP, IP, ICMP = connectionless – "best effort"

E. UDP
   1. Not reliable, less overhead

F. Internet, extranet, intranet

G. Electronic Data Interchange (EDI)
   1. Standardized way to communicate
   2. Standard forms
   3. VAN (Value Added Network)

H. Coaxial cable
   1. More resistant to interference than twisted pair

I. Baseband = one channel

J. Broadband = more than one channel

K. STP = less vulnerable to interference, cross talk, and eavesdropping

L. UTP = least secure
   1. Attenuation, crosstalk

M. Fiber = extremely resistant to eavesdropping, most secure, very expensive

N. Attenuation = loss of signal strength

O. Cross talk = signal spills over to another wire – UTP most susceptible

P. Plenum-rated cables = do not release dangerous chemicals when burned – used in plenum area

Q. Synchronous communication = no start and stop bits

R. Asynchronous communication = start and stop bits

S. Full versus partial mesh

T. Ethernet = shared media, broadcast, CSMA/CD, 802.3 ([illegible] – [illegible])

U. CSMA/CD = listens CSMA/CA = sends message

V. Token passing – control frame = token

- 1. Avoids collision
- 2. Token Ring, FDDI, ARCnet

W. Polling – primary asks secondary
- 1. HDLC, SDLC

X. ARP = IP to MAC mapping table (poisoning/MAC spoofing)

Y. RARP = MAC to IP mapping

Z. Repeater and hub = physical, amplifies signal

AA. Bridge = Forwards broadcasts, data link layer

BB. Switch = logical connection to each node, data link layer
- 1. Harder to sniff

CC. Router = network layer, does not forward broadcasts

DD. Brouter = IP address then MAC

EE. Gateway = software translator

FF. Firewall = chokepoint
- 1. Proxy = middle man – breaks connection
  - a. Application = looks deep into packet, one proxy per protocol or service
  - b. Circuit = more flexible, looks at less information than application
    - i. SOCKS
- 2. Stateful = builds a state table, tracks network conversations

GG. Bastion host = locked down system / 1st device [illegible]

HH. DMZ = buffer zone between untrusted and trusted

II. Screened host firewall = one screening firewall

JJ. Screened subnet firewall = two screening firewalls

KK. Dual-homed firewall = two NICs
- 1. Forwarding and routing needs to be disabled

LL. VPN = tunnel
- 1. IPSec
  - a. Allows for multiple connections
  - b. Tunnel mode = protect payload and headers
  - c. Transport mode = protect payload
- 2. PPTP
  - a. Works only over IP ([illegible])
- 3. L2TP
  - a. No encryption must be used with IPSec

MM. Serial Line Internet Protocol (SLIP)
- 1. Encapsulates data over a serial line
- 2. Replaced by PPP
- 3. No header and data compression
- 4. Works only with IP traffic

NN. Point to Point Protocol
- 1. Encapsulates data over a serial line
- 2. Authentication
  - a. Password Authentication Protocol (PAP)
    - i. Credentials in clear text

b. Challenge Handshake Authentication Protocol (CHAP)

i. Challenge value sent

ii. Password not sent over the wire

c. Extensible Authentication Protocol (EAP)

OO. Fiber Distributed Data Interface (FDDI)

1. Token passing, 100 Mbps, MAN, dual rings

PP. SONET

1. Self healing, dual rings

QQ. ISDN

1. BRI = 2 B and 1 D channels
2. PRI = 23 B and 1 D channels

RR. S/WAN = VPN

SS. DSL = "always on", digital local loop

TT. Cable modem = neighbors share same media – sniffing

UU. Circuit switching = voice, follows one path

VV. Packet switching = data, bursty traffic, packets follow different paths

WW. Frame Relay

1. Permanent virtual circuit (PVC) – permanent
2. Switched virtual circuit (SVC) – dynamic
3. Committed Information Rate (CIR) = ensures an amount of bandwidth

XX. X.25

1. First packet switching technology
2. Slower than frame relay and ATM because of amount of overhead required

YY. ATM = 53-byte fixed cells, cell switching, fast

ZZ. Packet switching technologies

1. Switched Multimegabit Data Service (SMDS)
2. Frame Relay

AAA. Remote Access

1. Call back number
   a. Call forwarding circumvents
2. Caller ID

BBB. RAID levels

1. Level 0 = striping
2. Level 1 = mirroring
3. Level 5 = parity over all disks

CCC. Server cluster

1. Fault tolerance

DDD. Phreakers

1. Red boxing = coins dropping
2. Blue boxing = tone manipulation

EEE. Wireless devices use Wireless Application Protocol (WAP) because of limited resources

1. WTLS has to be translated into TLS or SSL = "gap in the WAP"
2. Encryption in wireless = wired equivalent privacy (WEP)

[illegible] [illegible] context
switch [illegible]

3. War driving = picking up wireless signals, identifying Aps to access and attack network

IPV6 - 128 bits

VI. Operations Security

- A. Job rotation
  - 1. Reduces possible fraud
- B. Separation of duties
  - 1. Collusion
- C. Clipping level = threshold
- D. Dual control
  - 1. Two individuals to complete a task
- E. Library controls media access
- F. System recovery
  - 1. Must return to a more secure state
- G. Facsimile security
  - 1. Fax encryptor = encrypts bulk data at data link layer
- H. Operational duties
  - 1. Unusual or unexplained occurrences
  - 2. Deviations from standards
  - 3. Unscheduled Initial Program Loads
- I. Intrusion Detection System (IDS)
  - 1. Host-based
  - 2. Network-based
  - 3. Signature-based
  - 4. Behavior-based (Statistical & Anomaly)
    - a. Higher false-positives
    - b. Also called statistical and anomaly-based systems

VII. Applications and System Development

- A. Project development
  - 1. Project initiation
    - a. Identify security risks
    - b. Initial risk analysis
    - c. SLA
  - 2. Functional Design Analysis and Planning
    - a. Define security requirements
    - b. Preliminary security test plans
    - c. Security baseline
  - 3. System design specifications
    - a. Define secure specifications
    - b. Design checklist
  - 4. Software development
    - a. Write code
    - b. Unit tests
  - 5. Installation\test\implementation
    - a. Test

        - b. Implement
        - c. Create manuals
        - d. Certification and accreditation
    - 6. Operational/Maintenance
        - a. Maintain
        - b. Any changes = recertification, re-accreditation
    - 7. Disposal
- B. Change control
    - 1. Changes approved, tested, and recorded
- C. Library = centrally controlling software and changes
- D. Separation of duties
    - 1. Programmer does not change code in production
    - 2. Programmer is not the only one testing code
    - 3. Production code only comes from library
- E. Split knowledge procedures
    - 1. No one person has too much knowledge
- F. Object-oriented programming
    - 1. More efficient, re-use code
    - 2. Object = instance of a class
    - 3. Message = objects communicate
    - 4. Method = command object performs
    - 5. Abstraction = hiding details
    - 6. Polymorphism = two objects receive the same data and react differently
    - 7. Polyinstantiation = two, or more, copies of an object that holds different data
    - 8. Cohesive = level of object independence
    - 9. Coupling = level of activity between objects
    - 10. Java applet = sandbox
    - 11. ActiveX = public key cryptography
- G. Databases
    - 1. Relational = tables
        - a. Row = tuple
        - b. Column = attribute
        - c. Data dictionary = central repository – meta-data
        - d. Primary key = unique per row, links values in row
        - e. Foreign key = attribute in one table is the same as a primary key in another table
    - 2. Hierarchical = logical tree, parents and children
    - 3. Distributed = different places
    - 4. Concurrency = integrity
        - a. Rollback = return to earlier state
        - b. Commit = accept changes
        - c. Checkpoint = periodically saving data
    - 5. Aggregation

a. Access to some components and coming up with the full picture

6. Inference
   a. Deducing information not explicitly available
7. Data warehousing
   a. Data from several databases and presented in useful form
8. Data mining
   a. Finding patterns

H. Expert systems

1. Mimic human logic
2. Knowledge-based system
3. Rule-based programming – if/then
4. Inference engine – pattern matching

I. Artificial Neural Networks

1. Model after brain – units mimic neurons

J. Attacks

1. Smurf = broadcast, spoofed ICMP
2. Fraggle = broadcast, spoofed UDP
3. SYN = DoS
4. Timing
   a. Between the lines = tap into an active line
   b. NAK/ACK = unprotected during asynchronous interrupt
   c. Line disconnect = user ends session

K. Malware

1. Virus = cannot reproduce on own
2. Worm = can reproduce on own
3. Macro virus = easy to create because of the simplicity of the macro languages
4. Boot sector virus = malicious code inserted into disk boot sector
5. Compression virus = when decompressed it initializes
6. Stealth virus = hides its footprints and changes that it has made
7. Polymorphic virus = makes copies and changes the copies in some way
8. Multipartie virus = infects both boot sector and hard drive
9. Self-garbling virus = garbles own code to elude detection

VIII. Security Architecture and Models

A. Memory hardware segmentation provides more protection than logical controls

B. Compiler = all code turned into machine code

C. Interpreted code = one line of code turned and executed at a time

D. Layering = data hiding

E. Security domain = domain of execution

F. Trusted Computing Base = protection mechanisms, hardware, software, firmware

G. Security perimeter = imaginary boundary separating trusted and untrusted

H. Reference monitor = rules

I. Security kernel = rule enforcer

J. Single state machine = one security level

K. Multistate machine = multiple security levels

L. Bell-LaPadula – first mathematical state model dealing with access

1. Confidentiality
2. Simple security property = no read up
3. Star property = no write down

M. Biba – integrity

1. Star integrity axiom = no write up
2. Simple integrity axiom = no read down

N. Clark Wilson – integrity

1. Access object through program – access triple
2. Separation of duties
3. Auditing

O. Goals of integrity

1. 1st = prevent unauthorized users from making improper modifications (Biba)
2. 2nd = maintain internal and external consistence of data and systems
3. 3rd = prevent authorized users from making improper modifications
4. Biba provides for 1st goal and Clark-Wilson provide for all 3

P. Brewer and Nash (Chinese Wall)

1. Dynamic access controls
2. Conflict of interest

Q. Noninterference model

1. Activities in higher level do not affect lower level environment

R. Trusted Computer System Evaluation Criteria (TCSEC)

1. Orange Book
   a. A Verified protection
   b. B Mandatory protection (security labels)
   c. C Discretionary protection
   d. D Minimal security
2. Red Book = networking

S. Information Technology Security Evaluation Criteria

1. Evaluates functionality and assurance separately

T. Common Criteria

1. International – combo of all
2. EAL ratings
3. Uses profiles

U. Certification = technical evaluation

V. Accreditation = management approval

W. Covert channels

1. Timing = subject modulating resources
2. Storage = subject at higher level writing to storage and lower level subject reading it

X. Backdoor = maintenance hook, trapdoor

Y. Buffer overflow = software not checking input length

IX. Physical Security

A. Internal partitions = does not go to ceiling

B. Lightning and electrical motors cause electromagnetic interference

C. Fluorescent lighting and electrical systems cause radio frequency interference

D. Spike = Momentary high voltage

E. Surge = prolonged high voltage

S's voltage

F. Fault = Momentary power out

G. Blackout = Prolonged loss of power

H. Sag = Momentary low voltage

I. Brownout = Prolonged power supply that is below normal voltage

J. Data processing environment

1. 70-74F/21-23C
2. Humidity = 45-60%
   a. Low = static electricity
   b. High = corrosion

K. Detectors

1. Optical - photoelectric = light blockage
2. Ionization = reacts to charged particles of smoke

L. Class A fire = common combustibles

1. Water. soda acid

M. Class B fire = liquid

1. Gas, CO2, soda acid

N. Class C fire = electrical

1. Gas, CO2

O. Detector placement

1. On and above suspended ceilings, below raised floors, air ducts

P. Replacement for Halon = FM200

Q. Wet pipe

1. Water in pipe

R. Dry pipe

1. Water not in pipe
2. Better for colder climates

S. Pre-action pipe

1. Delay before release of water
2. Used in data processing environments

T. Deluge

1. Dry pipe that lets out a lot of water

U. Cipher locks = keypad

V. Proximity device

1. Transponder = reader interrogates card

W. Fencing

1. 3-4 ft – deters casual trespassers

2. 6-7 ft – too high to climb easily
3. 8 ft with 3 strands of barbed wire – deter determined intruder

Z. Extinguishers
1. 50 ft within electrical equipment
2. Quarterly inspection

X. Computer Law, Investigations and Ethics

A. Salami
1. Carrying out smaller crimes with the hope that the larger crime goes unnoticed

B. Data diddling
1. Altering data before it is inputted into a program or after it is outputted

C. Password sniffing
1. Capture passwords as they travel over a network

D. IP spoofing
1. Use a bogus IP address to hide identity

E. Dumpster diving
1. Go through trash in hopes of finding useful information
2. Not illegal

F. Pseudo flaw
1. Code in operating system or application inserted to trap intruders

G. Superzapper
1. Utility that can bypass access controls and make changes not detected by auditing tools

H. Transborder information flow
1. Abiding by different laws when passing data through different countries
2. Privacy of personal information

I. Civil law – tort
1. Wrongs against individuals
2. No jail time

J. Criminal law
1. Laws to protect public

K. Administrative law
1. Regulations

L. Trade Secret
1. Proprietary intellectual property

M. Copyright
1. Expression of ideas, not ideas themselves

N. Patent
1. Invention

O. Evidence
1. Life cycle