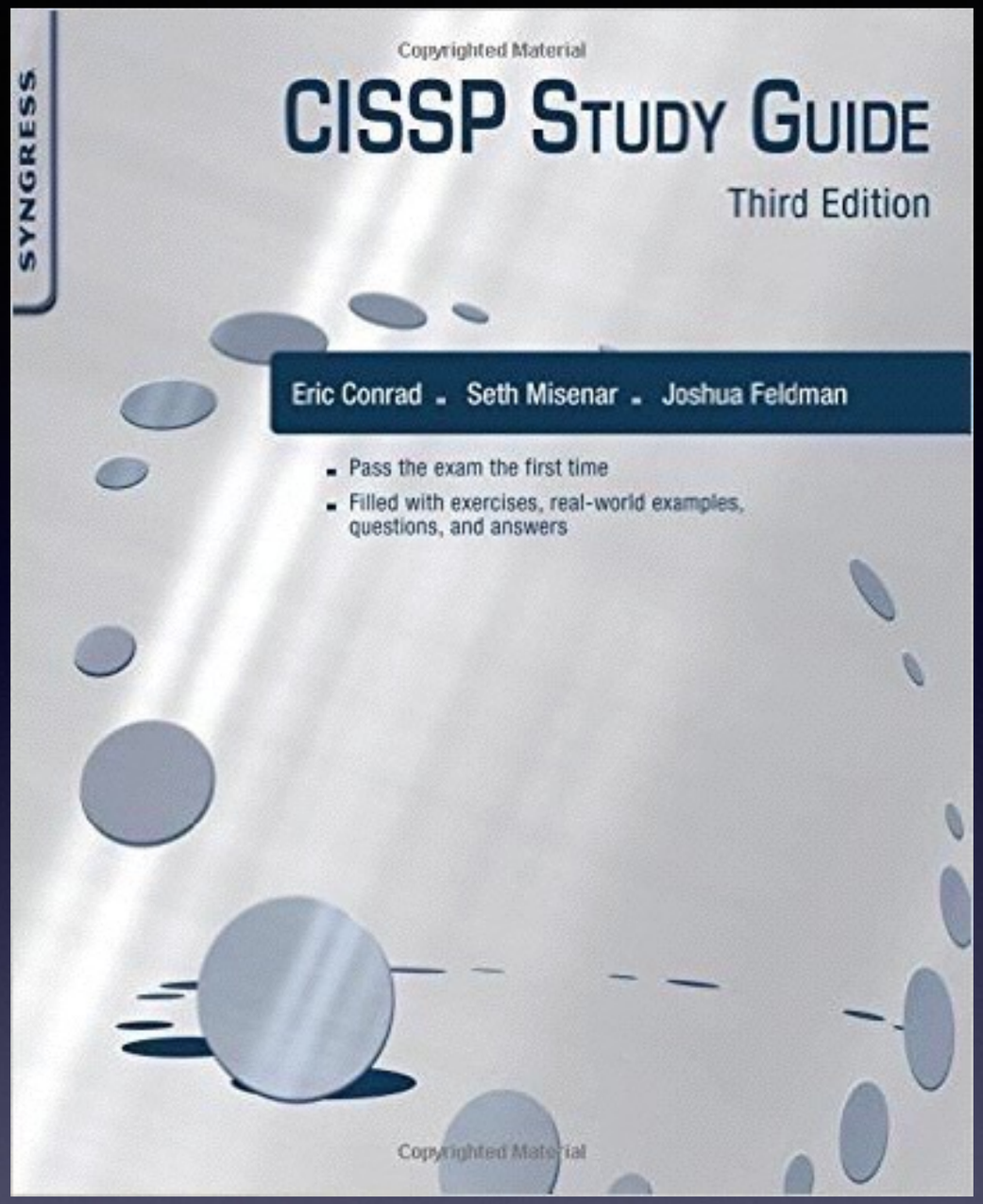
CNIT 125: Information Security Professional (CISSP Preparation)



Updated 10-13-17

Ch 2. Security and Risk Management (Part 2)

Legal and Regulatory Issues

Major Legal Systems

- **Civil Law**
  - Laws and statutes determine what is allowed
  - Precedents and particular case rulings carry less weight than under **common law**
- **Common Law**
  - Used in the USA, Canada, the UK, and former British colonies
  - Significant emphasis on particular cases and precedents as determinants of laws
  - The major legal system in the CISSP exam

Religious and Customary Law

- **Religious Law**
  - Mainly *Sharia* (Islamic religious law)
- **Customary Law**
  - Customs or practices that are commonly accepted and treated as law
  - Closely related to **Best Practices**
  - Less important

Criminal and Civil Law

- **Criminal Law**
  - Victim is society itself
  - Enforced by police
  - Punishment is often prison time
  - Proof must be beyond a reasonable doubt
- **Civil Law (Tort Law)**
  - Injury resulting from failure to provide due care
  - Victim is an individual
  - Enforced by lawsuits
  - Result is financial damages paid to victim
  - Burden of proof: **preponderance of the evidence** (more likely than not)

Table 2.1

Common Types of Financial Damages

Financial Damages	Description
Statutory	Statutory damages are those prescribed by law, which can be awarded to the victim even if the victim incurred no actual loss or injury.
Compensatory	The purpose of compensatory damages is to provide the victim with a financial award in effort to compensate for the loss or injury incurred as a direct result of the wrongdoing.
Punitive	The intent of punitive damages is to punish an individual or organization. These damages are typically awarded to attempt to discourage a particularly egregious violation where the compensatory or statutory damages alone would not act as a deterrent.

Administrative Law

- Also called **Regulatory Law**
- Specify rules and punishments for regulated industries
- Examples
  - FCC regulations
  - HIPAA security mandates
  - FDS regulations
  - FAA regulations

Liability

- Due Care
  - Also called **Duty of Care**
  - **Prudent Man Rule**
    - Businesses should do what a prudent man would do
  - Best Practices
- Due Diligence
  - The management of due care
  - Follows a formal process

Legal Aspects of Investigations

Evidence

- **Real evidence**
  - Physical objects like hard drives, USB drives, etc.
- **Direct evidence**
  - Witness testimony about what that person experienced directly
- **Circumstantial evidence**
  - Indirect evidence of guilt
  - Can support other evidence, but usually inadequate for conviction alone

Evidence

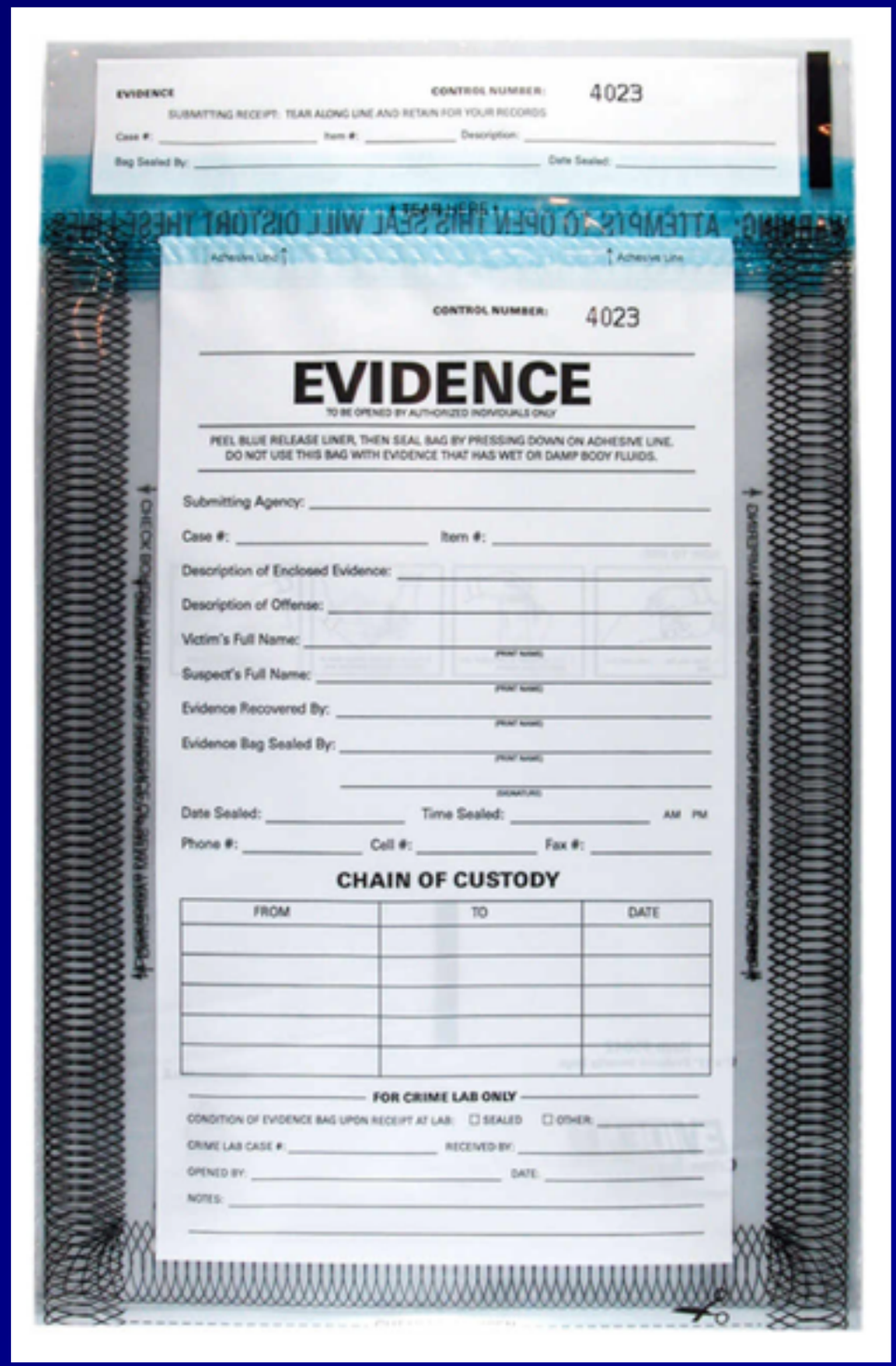
- **Corroborative evidence**
  - Additional support for a fact that may be called into question
- **Hearsay**
  - Secondhand evidence
  - Normally inadmissible in court
  - Exceptions:
    - Business records and computer-generated evidence
  - Computer forensic hard disk and memory images are original evidence, not hearsay

Evidence

- **Best evidence**
  - Original documents, not copies
  - The actual hard drive used
  - Etc.
- **Secondary evidence**
  - Copies of documents
  - Log files may be considered secondary or original
- **Evidence integrity**
  - Typically ensured by MD5 or SHA-1 hash

Chain of Custody

- Evidence must be protected from tampering
- A list of names of people who can testify that they protected the evidence



Reasonable Searches

- Fourth amendment protects citizens from unreasonable search and seizure by the government
- Illegally obtained evidence is inadmissible in court
- Most searches require **probable cause** and a **search warrant**

Exceptions

- These searches don't require a warrant
  - Objects in plain sight
  - At a public checkpoint
  - Exigent circumstances
    - Immediate threat to human life or of evidence being destroyed

Agents of Law Enforcement

- Private citizens are not part of the government, so the fourth amendment does not apply, unless:
- Private citizens who carry out investigations on behalf of law enforcement, they are acting **under the color of law enforcement** or **agents of law enforcement**
- Then the fourth amendment applies

Should You Call Law Enforcement?

Note

Due to the particular issues unique to investigations being carried out by, or on behalf of, law enforcement, an organization will need to make an informed decision about whether, or when, law enforcement will be brought in to assist with investigations.

- Companies often avoid involving law enforcement
- Makes cases simpler, avoids publicity

Entrapment and Enticement

- **Entrapment**
  - Law enforcement agent persuades someone to commit a crime when
  - The person otherwise had no intention to commit a crime
- **Enticement**
  - Law enforcement agent makes conditions favorable for a crime
  - Person is already intent on committing a crime

Computer Crime

- Computer as **target**
  - DoS, installing malware to send spam
- Computer as a **tool**
  - Stealing secrets from a database
  - Stealing credit card numbers
  - Espionage
  - Harassment
- **Attribution**
  - Difficult to prove who did a crime

Intellectual Property

- **Trademark**
  - Name, logo, or symbol used for marketing
  - Unregistered ™ or Registered ®
- **Patent**
  - Grants a monopoly for an invention
- **Copyright ©**
  - Restricts copying creative work
  - Software typically covered by copyright
  - **Fair sale** & **fair use** are allowed

Intellectual Property

- **Licenses**
  - End-User License Agreement (EULA)
- **Trade secrets**
  - Special sauce
  - Protected by non-disclosure agreements (NDAs) & non-compete agreements (NCAs)

Intellectual Property Attacks

- Software piracy
- Copyright infringement
- Corporate espionage
- Cybersquatting & Typosquatting
  - Using a domain close to a company's domain, like *yahoo.net* or *yahooo.com*

Privacy

- Confidentiality of personal information
- **EU Data Protection Directive**
  - Individuals must be notified how their data is used & allowed to opt out
- **OECD Privacy Guidelines**
  - Organization for Economic Cooperation and Development
  - Includes EU, USA, Mexico, AU & more

EU-US Safe Harbor

- Part of EU Data Protection Directive
- Sending personal data from EU to other countries is forbidden
  - Unless the receiving country adequately protects its data
- The USA **lost** this privilege in Oct. 2015 because of the Snowden leaks

Privacy Shield

- Replaced Safe Harbor
- Approved by the EU in 2016 and Switzerland in 2017
  - Links Ch 2g, 2h, 2i

International Cooperation

- Council of Europe Convention on Cybercrime
  - Includes most EU countries and the USA
  - Promotes cooperation

Import / Export Restrictions

- USA restricted exports of cryptographic technology in the 1990s
- Restrictions have been relaxed since then

Kahoot!

Important Laws and Regulations

HIPAA

- Health Insurance Portability and Accountability Act
- Guidance on Administrative, Physical, and Technical safeguards
- For Protected Health Information (PHI)

CFAA

- Computer Fraud and Abuse Act
- Protects government and financial computers
  - Including every computer on the Internet (probably not the law's original intent)
- It's a crime to exceed your authorization to use such a computer

ECPA & The PATRIOT Act

- Electronic Communications Privacy Act
- Protected electronic communications from warrantless wiretapping
- Weakened by the PATRIOT Act
- The PATRIOT Act
  - A response to 9/11 attacks
  - Greatly expanded law enforcement's electronic monitoring capabilities

GLBA & SOX

- Gramm-Leach-Bailey Act
  - Forces financial institutions to protect customer financial information
- Sarbanes-Oxley Act
  - Response to ENRON scandal
  - Regulatory compliance mandates for publicly traded companies
  - Ensures financial disclosure and auditor independence

PCI-DSS

- Payment Card Industry Data Security Standard
- Self-regulation by major vendors
- Mandates security policy, devices, controls, and monitoring to protect cardholder data

US Breach Notification Laws

- 47 states require notification
- No federal law yet
- Safe harbor for data that was encrypted at time of compromise

Security and 3rd Parties

Service Provider Contractual Security

- Service Level Agreements (SLA)
  - Identify key expectations vendor must meet
- Attestation
  - Third party review of the service provider to determine security posture
  - Includes SAS 70 (old), ISO 27001, and PCI-DSS

Pentests & Procurement

- Right to Penetration Test / Audit
  - Allows the originating organization to perform these security tests on a vendor
- Procurement
  - Purchasing products or services
  - Considering security before purchase is best

Other Concepts

- Vendor Governance
  - Ensure that vendor provides sufficient quality
- Acquisitions
  - Purchasing a company to add to an existing company
  - Can disrupt security
- Divestitures
  - Splitting a company into parts
  - May result in duplicate accounts and other risks

Ethics

(ISC)^2 Code of Ethics

- Four Canons
  - Protect society, the commonwealth, and the infrastructure
  - Act honorably, honestly, justly, responsibly, and legally
  - Provide diligent and competent service to principals
  - Advance and protect the profession

Ethics Complaint

(ISC)²

29 September 2011

Mr. Sam Bowne

[redacted]

SENT VIA: ***USPS Certified Mail***
Return Receipt Requested

RE: Ethics Complaint

Dear Mr. Bowne:

This letter serves as notice to you that (ISC)² is in receipt of a formal ethics complaint that has been filed against you.

Accusation

On June 28, 2011, I was reading the ccsf.edu site to learn more about Sam Bowne's role at the college. During the course of normal browsing, I found several concerns on the web site that had serious security concerns. What I observed indicated the possibility a system had been compromised, or was potentially misconfigured in such a way as to mislead visitors into providing sensitive data from third-party sites. Knowing that Bowne is a professor at the college, I asked him through public Twitter messages and direct messages who I should contact, and did not receive reply.

9:51 PM Jun 27th to sambowne - I am serious. Can I get a security contact for ccsf.edu please? Ran into what I consider a serious issue on the web site.
10:11 PM Jun 27th from sambowne - Please tell me what you have found.
10:17 PM Jun 27th to sambowne - I cannot validate that you are the appropriate security contact for the City College of San Francisco.

I called the college directly and received two security contacts in their IT department that would handle security concerns. Neither of those contacts were Sam Bowne. When I emailed the two contacts to provide the information regarding their web site, I also asked if Bowne was a legitimate security contact for such issues. Tim Ryan, Technical Operations Manager for City College of SF (ccsf.edu) indicated that Bowne "is a Faculty Member in our academic Computer Networking Department (CNIT), he is not part of our internal security team".

Sam Bowne misrepresented himself as being a security contact for his university, when he was not. In

Verdict

FINDINGS:

While the Complainant accuses the Respondent of misrepresenting his role with his employer, he does not provide any evidence supporting such a claim. Complainant further claimed that Respondent discontinued communication with Complainant; however, we can find no duty incumbent upon the Respondent to respond to Complainant. It is also noted that Complainant admits in his complaint that he "called the college directly and received two security contacts."

RECOMMENDATION

It is the unanimous recommendation of the Ethics Committee that the $(ISC)^2$ Board of Directors dismiss the complaint with prejudice.

RESPECTFULLY SUBMITTED,

(ISC) ETHICS COMMITTEE
18 November 2011

Information Security Governance

Table 2.3

Summary of Security Documentation

Document	Example	Mandatory or Discretionary?
Policy	*Protect the CIA of PII by hardening the operating system*	Mandatory
Procedure	*Step 1: Install pre-hardened OS Image. Step 2: Download patches from update server. Step 3: …*	Mandatory
Standard	*Use Nexus-6 laptop hardware*	Mandatory
Guideline	*Patch installation may be automated via the use of an installer script*	Discretionary
Baselines	*Use the CIS Security Benchmarks Windows Benchmark*	Discretionary

Personnel Security

- Security Awareness and Training
- Background Checks
- Employee Termination
  - Must use fair process
- Vendor, Consultant and Contractor Security
- Outsourcing and Offshoring
  - Can lower Total Cost of Ownership
  - May improve security
  - Privacy and regulatory issues
  - Must perform risk analysis first

Kahoot!

Access Control Defensive Categories and Types

Access Control Types

- Preventive
- Detective
- Corrective
- Recovery
- Deterrent
- Compensating

Access Control Types

- Preventive
  - Prevents actions, such as limited privileges
- Detective
  - Alerts during or after an attack, like video surveillance
- Corrective
  - Corrects a damaged system or process, like antivirus removing a suspicious file

Access Control Types

- Recovery
  - Restores functionality after a security incident, such as restoring from backups
- Deterrent
  - Scares away attackers, like a "Beware of Dog" sign
- Compensating
  - Additional control to compensate for weakness in other controls
  - e. g. reviewing server logs to detect violations of the Computer Use Policy (an administrative control)

Access Control Categories

- Administrative
  - Policy, procedure, or regulation
- Technical
  - Software, hardware, or firmware
- Physical
  - Locks, security guards, etc.

Here are more clear-cut examples:

- Preventive
  - Physical: Lock, mantrap
  - Technical: Firewall
  - Administrative: Pre-employment drug screening
- Detective
  - Physical: CCTV, light (used to see an intruder)
  - Technical: IDS
  - Administrative: Post-employment random drug tests
- Deterrent
  - Physical: "Beware of dog" sign, light (deterring a physical attack)
  - Technical: Warning Banner presented before a login prompt
  - Administrative: Sanction policy

Risk Analysis

Risk Analysis

- Assets
  - Valuable resources to protect
- Threat
  - A potentially harmful occurrence
- Vulnerability
  - A weakness

Risk = Threat x Vulnerability

- Earthquake risk is the same in Boston and San Francisco
- Boston
  - Earthquakes are rare, but buildings are old and vulnerable
- San Francisco
  - Earthquakes are common, but buildings are newer and safer

Impact

- Severity of the damage in dollars
- Risk = Threat x Vulnerability x Impact
- Human life is considered near-infinite impact

Table 2.4

Risk Analysis Matrix

		Consequences				
		Insignificant 1	Minor 2	Moderate 3	Major 4	Catastrophic 5
Likelihood	5. Almost Certain	H	H	E	E	E
	4. Likely	M	H	H	E	E
	3. Possible	L	M	H	E	E
	2. Unlikely	L	L	M	H	E
	1. Rare	L	L	M	H	H

Table 2.5

Summary of Risk Equations

	Formula	Description
Asset Value (AV)	**AV**	Value of the Asset
Exposure Factor (EF)	**EF**	Percentage of Asset Value Lost
Single Loss Expectancy (SLE)	**AV x EF**	Cost of One Loss
Annual Rate of Occurrence (ARO)	**ARO**	Number of Losses per Year
Annualized Loss Expectancy (ALE)	**SLE x ARO**	Cost of Losses per Year

Total Cost of Ownership (TCO)

- Of a mitigating safeguard includes
  - Upfront costs
  - Annual cost of maintenance
    - Staff hours
    - Maintenance fees
    - Software subscriptions

Return on Investment (ROI)

- Amount of money saved by implementing a safeguard
- If Total Cost of Ownership is less than Annualized Loss Expectancy, you have a positive ROI

Risk Choices

- Accept the risk
- Mitigate the risk
- Transfer the risk
- Risk avoidance

Quantitative and Qualitative Risk Analysis

- Quantitative
  - Uses hard metrics, like dollars
- Qualitative
  - Use simple approximate values
  - Or categories like High, Medium, Low

NIST 9-Step Risk Analysis Process

1. System Characterization
2. Threat Identification
3. Vulnerability Identification
4. Control Analysis
5. Likelihood Determination
6. Impact Analysis
7. Risk Determination
8. Control Recommendations
9. Results Documentation

Types of Attackers

Types of Attackers

- Hackers
  - Black hat, white hat, gray hat
- Script kiddies
- Outsiders
  - Outside the company
- Insiders
- Hacktivists
- Bots
- Phishing


Kahoot!