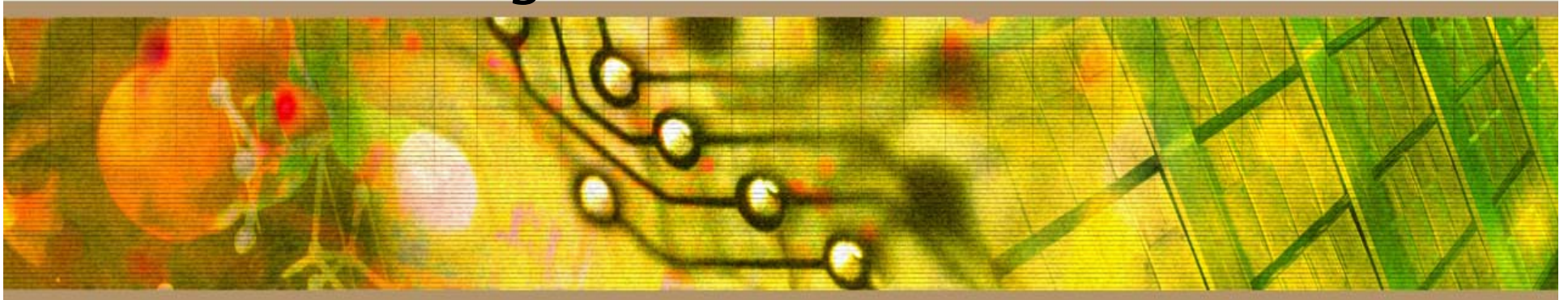




ITNS and CERIAs
CISSP Luncheon Series:
Legal, Regulations, Compliance, and
Investigations



Presented by Joanna L. Grama, J.D., CISSP



- From (ISC)2 Candidate Information Bulletin:
 - The Legal, Regulations, Compliance and Investigations domain addresses computer crime laws and regulations; the investigative measures and techniques which can be used to determine if a crime has been committed, methods to gather evidence if it has, as well as the ethical issues of code and conduct for the security professional. Incident handling provides the ability to react quickly and efficiently to malicious threats or incidents.

- From (ISC)2 Candidate Information Bulletin:
 - The candidate will be expected to know the methods for determining whether a computer crime has been committed; the laws that would be applicable for the crime; laws prohibiting specific types of computer crime; methods to gather and preserve evidence of a computer crime; investigative methods and techniques; and ways in which RFC 1087 and the (ISC)2 Code of Ethics can be applied to resolve ethical dilemmas.

- Why do we care about this?
 - Computer is a tool that can be used for good or evil.
 - Computers bring new opportunities for thieves and crooks.
 - » This can raise questions of jurisdiction.
 - Legal issues are important to a company because a violation of laws can be damaging to the company's bottom line and reputation.

- Major types of legal systems
 - Common law
 - Civil or code law
 - Customary law
 - Religious law
 - Mixed law

■ Common Law

- Traces its roots back to England, framework can be found in many countries that were once colonies of the British Empire
- Notable for its adversarial approach
- Based on the notion of precedent
- Three types of branches:
 - » Criminal
 - » Tort
 - » Administrative

- Civil Law
 - Roots in Roman Empire and Napoleonic Code of France
 - Used in parts of Europe and Asia
 - Primary characteristic is the codification of law and heavy reliance on legislation as the primary source of law.

- Customary Law
 - Reflect society's norms and values based on programmatic wisdom and traditions.
 - Customs have created legitimate social contracts that are legally enforceable.
 - Most countries that use customary law pair it with another type of legal system.

- Religious Law
 - Law is not considered man-made, but is decreed by divine will.
 - Some systems have codified this type of law (e.g., the Sharia in traditional Islamic law).
 - Jurists and clerics play a central role and have a high degree of authority within the society.

- **Mixed Law**
 - The blending of two or more systems of law.
 - Is becoming increasingly common as the world is more globalized.
 - Traditional mix is common law + code law; but religious law + code law/common law is becoming more common.

- Intellectual Property Laws
 - Patent
 - Trademark
 - Copyright
 - Trade Secret
 - Licensing Issues
- Privacy
- Liability
- Computer Crime

- Intellectual property laws address how a company or person can protect what it rightfully owns, and what it can do if those rights are violated.
- Protects both tangible and intangible types of property.
- IP laws vary from country to country.

■ Patents

- Patents are granted to inventors to keep others from using the invention covered for a period of time (e.g., usually 20 years).
- Protects novel, useful, and nonobvious inventions.
- Many different types of items can be patented: mechanical items, pharmaceuticals, algorithms

- Trademark
 - Creates exclusive rights to the owner of markings that the public uses to identify various vendor/merchant products or goods.
 - A trademark consists of any words, names, product shape, symbol, color, or a combination of these used to identify products or a company.
 - Think marketing and branding issues.

- Copyright
 - Used to protect the expression of an idea.
 - In most countries (and in the US), copyright protection is automatically assumed once the work or property is completed and in tangible form. (But enforcement is another issue if not registered.)
 - Can be used to protect source code.
 - Is weaker protection than patent or trademark, but protection is longer (75 years in U.S.)

- Trade Secret
 - Deemed proprietary to a company, and often include information that provides a competitive edge (e.g., Coca-Cola formula, the Colonel's Secret Recipe, source code, etc.)
 - These are protected when employers require employees to sign non-disclosure agreements.
 - Company's must take steps to protect.

- Licensing Issues
 - Concerns the use of illegal software or piracy.
 - 4 Categories of software licenses: freeware, shareware, commercial, & academic.
 - Most common agreements are “Master Agreements” and “EULAs.”

■ Privacy Issues

- “The rights and obligations of individuals and organizations with respect to the collection, use, retention, and disclosure of personal information.
- Balance between protecting a citizen’s information and business/government need for information.
- Depth of privacy legislation depends on jurisdiction.
- Horizontal Enactment: Generic requirements across all industries, including government
- Vertical Enactment: Regulate by industry (health care, financial, industry)

- Privacy is recommended as a fundamental right in many nations
 - United Nations Declaration of Human Rights
 - US Privacy Act of 1974
 - European Union Principles
 - International Covenant on Civil and Political Rights
 - Organization for Economic Cooperation and Development
 - Safe Harbor Act

- Privacy Issues

- Know the Organization for Economic Co-operation and Development (OECD) guidelines:
 - » Collection Limitation
 - » Data Quality
 - » Purpose Specification
 - » Use Limitation
 - » Security Safeguards
 - » Openness
 - » Individual Participation
 - » Accountability

- Privacy in the Workplace
 - Employee electronic monitoring
 - Email monitoring
 - Document monitoring
 - Internet activity monitoring
 - Personally identifiable information

- Liability
 - If a company does not practice *due care* in its efforts to protect itself from computer crime, it can be found to be negligent and legally *liable* for damages.
 - Liability is typically based on a negligence action.

- Core concepts:
 - Due Diligence
 - Due Care
 - Prudent Person Rule (it's a legal fiction)

- Computer Crime
 - Computers are now the targets of many criminals.
 - Computer crimes can be divided into three categories:
 - » Computer as a tool
 - » Computer as the target of the crime
 - » Computers incidental to the crime

- Computer Crime
 - Biggest hurdle to combating computer crime is its international flavor.
 - There are no borders in cyberspace.
 - Domestic laws cannot address the problem
 - Council of Europe (CoE) Cybercrime Convention
 - » Includes European countries, the US, Canada, and China.

- Computer Forensics
 - Starts to deal with evidence and the legal system
 - Generic Forensics Model for all Evidence:
 - » Identifying Evidence
 - » Collecting Evidence
 - » Examining Evidence
 - » Presentation of Findings

- Computer Forensics
 - Evidence at the Crime Scene:
 - » Identify the scene
 - » Protect the environment
 - » Identify evidence and potential sources of evidence
 - » Collect evidence
 - » Minimize evidence contamination.

- 5 rules of evidence of all types:
 - Authentic
 - Accurate
 - Complete
 - Convincing
 - Admissible

- Chain of custody is important!

- Incident Response
 - Simple definition: “The practice of detecting a problem, determining its cause, minimizing the damage it causes, resolving the problem, and documenting each step of the response for future reference.”
 - Common framework for incident response:
 - » Creation of a response capability
 - » Incident response and handling
 - » Recovery and feedback

- Goals of Incident Response
 - Reduce potential impact to organization through effective and efficient response
 - Provide management with sufficient information to decide appropriate course of action
 - Maintain or restore business continuity
 - Defend against more attacks
 - Deter attacks through investigation and prosecution.

- Response Capability
 - Foundation for the incident response program includes organizational policies and procedures.
 - Policy must be clear, delegate authority to the incident response team, provide escalation procedures, and delineate communications procedures.
 - This all needs to be done before an incident.

- Response Capability
 - Also must have an IT team.
 - Many different models for team composition.
 - » Virtual Teams
 - » Permanent Teams
 - » Hybrid Teams
 - Core areas of the organization should be represented on the IR team.

- Incident Response and Handling
 - Methodical approaches required.
 - Basic model of incident response and handling:
 - » Triage
 - » Investigation
 - » Containment
 - » Analysis and Tracking
 - » Recovery
 - » Debriefing and Feedback

- (ISC)2 requires all CISSPs to commit to fully supporting its Code of Ethics.
- Other quasi-governmental bodies with underlying ethical structures:
 - Computer Ethics Institute
 - » “Ten Commandments of Computer Ethics”
 - Internet Architecture Board

- (ISC)2 Code of Ethics
 - Canons:
 - » Protect society, the commonwealth, and the infrastructure.
 - » Act honorably, honestly, justly, responsibly, and legally.
 - » Provide diligent and competent service to principles.
 - » Advance and protect the profession.