# Digital Crime and Security Practices

## CISSP Study Guide - X

# Introduction to Digital Crime and Security Practices

- **Overview of Security Practices Influenced by Law**

> - Organizations adopt security measures based on legal requirements.
> - Liability in digital crime determined by law adherence during investigation.
> - In the U.S.A., the Secret Service and the FBI handle computer crime investigations.

- **Internal Threats and Protection Measures**

> - Most security breaches involve internal actors; disgruntled employees pose a high risk.
> - Security professionals are tasked with device updates to prevent attacks.
> - Emphasis on due care and diligence within a comprehensive security strategy.

- **Incident Reporting Systems**

> - Essential to provide safe channels for employees to report crimes.
> - Cultural barriers to incident reporting include fear of involvement or wrongful accusation.

# Categories of Digital Crime

- **Computer-Assisted Crime**

> - Utilizes computers as tools to facilitate traditional crimes.
> - Can occur without computers but simplified by technological means.

- **Computer-Targeted Crime**

> - Direct attacks on computers aimed at damaging the systems.
> - Examples include Distributed Denial of Service (DoS) and Buffer Overflow attacks.

- **Incidental Computer Crime**

> - Involves computers indirectly, possibly as a tool within a larger scheme.
> - For instance, computers used as part of a botnet.

- **Computer Prevalence Crime**

> - Arises exclusively due to widespread computer usage.
> - A typical example is software piracy.

# Understanding Major Legal Systems

### Civil Code Law vs. Common Law

- **Civil Code Law:** Rule-based law prevalent worldwide, not precedent-reliant.
- **Common Law:** Precedent-based, reflects societal morals, used in the US, UK, and others.

### Criminal, Civil/Tort, and Administrative Law

- **Criminal Law:** Actions harmful to society, possible fines, and imprisonment.
- **Civil/Tort Law:** Liability and damages such as economic, negligence, and nuisances.
- **Administrative Law:** Gov't standards for sectors like banking and healthcare.

# Intellectual Property and its Protection

## 1 Patents

- Exclusive rights for inventors to utilize and sell their inventions for a period, typically 20 years.

## 2 Trademarks

- Protect symbols or expressions from unauthorized use, significant for brand identity.

## 3 Copyrights

- Protect authored work from unauthorized reproduction, often life of author plus 70 years.

## 4 Trade Secrets

- Protect proprietary technical or business information, maintain confidentiality.

# Software Types and Piracy

- Understanding Software Licenses

> - Freeware, Shareware, and Commercial Software defined by usage and distribution rights.

- **Combating Software Piracy**

> - Security professionals must ensure staff education on the legal use of software.
> - Effective use of enterprise software for software installation monitoring.

- **Protecting Confidential Resources**

> - Secure access to intellectual properties like patents and copyrights.
> - Implement classification, access, and audit controls.

# Privacy and Information Protection

**Areas of Privacy Concern**

- Personal information sharing boundaries.
- Confidential message exchange.
- Anonymous communication possibilities.

**Protection of Personally Identifiable Information (PII)**

- Recognize and safeguard information that can uniquely identify an individual.
- Comply with international and domestic privacy laws and regulations.

# Key Laws and Regulations Affecting Security Practices

## 1 Comprehensive Compliance Mandates

- SOX Act, HIPAA, Gramm-Leach-Bliley Act set standards for financial and health data protection.

## 2 Security-Specific Legislation

- CFAA, Federal Piracy Act, and FISA define computer and communication-related offenses.

## 3 Data Security Standards

- PCI DSS requires annual compliance demonstration by entities handling cardholder information.

# Legal and Ethical Implications of Security Practices

- **Liability Management through Due Diligence and Care**

> - Legal responsibility from actions or negligence.
> - **Due diligence:** Understanding risks.
> - **Due care:** Implementing protections against risks.
> - Organizational negligence implications and necessity for proactive measures.

- **Criminal and Civil Penalty Exposure**

> - Senior management accountability for lawful practice and security issues.

# Incident Response and Handling

### Initiating Incident Investigation

- Define event versus an incident, focus on negative events impacting operations.
- Ensure evidence preservation and documentation.

### Incident Response Team and Protocols

- Define team roles, skill requirements, and response procedures.
- Establish evidence preservation along with legal authority interaction.

### Forensic and Digital Investigations

- Follow forensic guidelines to safeguard evidence admissibility.
- Steps include evidence identification to presentation and decision-making in the court proceedings.

# Professional Ethics in Security

## 1 Guidelines and Codes of Conduct

- (ISC)² Code of Ethics outlines responsibilities and conduct for certified professionals.
- Ten Commandments of Computer Ethics delineate respectful and responsible use of computers.

## 2 Ethical Responsibilities and Violations

- Reporting unethical actions among peers.
- Adhering to principles to advance and protect the profession.

## 3 Global Ethical Considerations

- Understanding and navigating ethical dynamics within international business environments.

# Information Security Buzz

**Discover more at our InfoSec Knowledge Hub**