MODULE 6: LEGAL, ETHICAL, AND PROFESSIONAL ISSUES IN INFORMATION SECURITY

INTRODUCTION TO LAW AND ETHICS IN INFORMATION SECURITY

InfoSec professionals must understand legal and ethical responsibilities tied to handling data.

- **Law** – enforced by the state; ethics: societal norms not legally binding.
- Ethics guide behavior even when no laws apply, both shape policymaking and operations.

Organizational Liability and the Need for Counsel

- Organizations can be **legally liable** for actions of employees even without criminal intent.
- Liability involves restitution and fines.
- Practicing **due care** (acting responsibly) and **due diligence** (maintaining that behavior) is essential to avoid legal exposure.

Policy Versus Law

- **Policy** – Internal rules within an organization; not enforceable by law but binding to employees.
- **Law** – Enforced by the government; failing to comply can result in prosecution or penalties.

Types of Law

1. **Statutory Law** – Created by legislative bodies.
2. **Regulatory Law** – Originates from executive/regulatory agencies.
3. **Common Law/Case Law** – Established by court precedents.

Categories of law

- **Civil Law**: Governs relationships between individuals/orgs (e.g., contract, tort).
- **Criminal Law**: Addresses offenses against the state/society.
- **Private Law**: Focuses on individual relationships.
- **Public Law**: Governs the state and its functions

RELEVANT U.S. LAWS

General Computer Crime Laws

- **Computer Fraud and Abuse Act (CFAA)** – Core U.S. law against hacking and data breaches.
- **USA PATRIOT Act** – Expanded government powers to combat cyber-terrorism.
- **PATRIOT Sunset Extension Act (2011)** – Extended surveillance provisions.

Privacy Laws

- **Federal Privacy Act of 1974** – Limits government's use of personal data.
- **Electronic Communications Privacy Act (1986)** – Protects electronic communications.
- **HIPAA (1996)** – Protects health information.
- **Gramm-Leach-Bliley Act (1999)** – Affects financial data handling.

Identity Theft

- Cybercrime laws penalize unauthorized use of personal data.
- Organizations must ensure strong safeguards to protect identities.

Export and Espionage Laws

- U.S. restricts export of encryption tech and certain security tools.
- **Espionage Act** and others apply when tech secrets are stolen or leaked abroad.

U.S. Copyright Law

- Protects digital and intellectual property.
- Includes software, documents, designs.
- Digital copies are protected like physical ones.

Financial Reporting Laws

- **Sarbanes–Oxley Act (2002)**: Holds executives accountable for financial data integrity.

- Information security is crucial for accurate financial reporting.

Freedom of Information Act (FOIA) of 1966

Citizens can request federal data—except confidential/national security materials.

Payment Card Industry Data Security Standards (PCI DSS)

- Not a law, but an enforced standard.
- Applies to all entities that handle cardholder data.
- 12 broad requirements including firewalls, access control, encryption, and monitoring.

State and Local Regulations

- Each U.S. state has its own data breach notification laws.
- Security professionals must stay informed of regional compliance needs.

INTERNATIONAL LAWS AND LEGAL BODIES

1. **U.K.**
   - **Computer Misuse Act (1990)**: Targets unauthorized access and malware.
   - **Police and Justice Act (2006)**: Updates to penalties and added offenses.
2. **Australia**
   - **Privacy Act (1988)**: Regulates personal data.
   - **Cybercrime Amendment Bill (2011)**: Aligns with EU Cybercrime Convention.
3. **Council of Europe Convention on Cybercrime**
   - First international treaty on cybercrime; encourages collaboration across borders.
4. **World Trade Organization / TRIPS**
   - Trade-Related Aspects of Intellectual Property Rights protect copyright, trademarks, and patents globally.
5. **Digital Millennium Copyright Act (DMCA)**
   - Prohibits bypassing digital rights management (DRM).
   - Also regulates tools/devices used to circumvent protections.

ETHICS AND INFORMATION SECURITY

InfoSec lacks universal binding ethical codes.

- Many orgs use "soft enforcement" through membership and certification requirements.
- Ten Commandments of Computer Ethics (e.g., don't snoop, steal, or harm using computers).

Ethical Differences Across Cultures

- Cultural norms affect interpretations of piracy and software sharing.
- Western individualism vs. Eastern collectivism causes conflict over intellectual property.

Ethics and Education

- Training and awareness programs foster good behavior.
- Ignorance of policy is a valid concern—requires proactive education.

Deterring Unethical and Illegal Behavior

- Three causes: **Ignorance**, **Accident**, **Intent**.
- Three deterrents: **Fear of penalty**, **Probability of apprehension**, **Likelihood of enforcement.**

CODES OF ETHICS OF PROFESSIONAL ORGANIZATIONS

Organization	Focus
ACM	Academic/professional ethics
ISACA	Auditing and control standards
ISSA	InfoSec best practices
(ISC)²	CISSP & SSCP certifications
SANS/GIAC	Technical certifications
EC-Council	CEH and CCISO ethics

Key U.S. Federal Agencies

1. **Department of Homeland Security (DHS)** – Coordinates cyber defense.
2. **U.S. Secret Service (USSS)** – Investigates financial cybercrimes.

3. **Federal Bureau of Investigation (FBI)** – Handles cyberterrorism and national security threats.
4. **National Security Agency (NSA)** – Signals intelligence and cryptography.

MODULE 7: SECURITY AND PERSONNEL

INTRODUCTION TO SECURITY AND PERSONNEL

Security success depends not only on technology but on proper personnel management.

- Changes in security can cause employee anxiety—organizations should perform a behavioral feasibility study to assess impact.
- Key question examples: "Will I be monitored?" "Will this affect my job performance?"

POSITIONING THE SECURITY FUNCTION

- Security can be positioned under:
  - CIO (Chief Information Officer)
  - CISO (Chief Information Security Officer)
  - Legal or Risk Management (for independence)
- Reporting structure should balance **authority, independence, and alignment with business goals**.

STAFFING THE INFORMATION SECURITY FUNCTION

- Requires collaboration among IT, HR, and management.
- Must assess:
  - Organizational needs
  - Cultural readiness
  - Strategic alignment
- Use of standard job descriptions increases professionalism.

Qualifications and Requirements

- Skills needed:
  - Tech knowledge
  - Business acumen
  - Communication skills
  - Policy awareness
  - Problem-solving ability
- Most valuable: **well-rounded generalist** over overspecialized technician.

Entry into the Information Security Profession

- Common entry paths:
  - Law enforcement/military
  - Traditional IT roles (sysadmin, developer)
  - Academic programs (increasing trend)
- Emphasis on role clarity and defined career paths.

Information Security Positions

- Roles classified into:
  - Definers – Managers, policy writers
  - Builders – Engineers, system architects
  - Administrators – Analysts, technicians
- Charles Cresson Wood's book offers model job descriptions.

CREDENTIALS FOR INFOSEC PROFESSIONALS

(ISC)² Certifications

- CISSP (Certified Information Systems Security Professional)
- SSCP (Systems Security Certified Practitioner)
- Associate of (ISC)²
- Concentrations in Architecture, Management, Engineering,

ISACA Certifications

- CISM (Certified Information Security Manager)
- CISA (Certified Information Systems Auditor)
- CRISC, CGEIT

SANS / GIAC Certifications

- GIAC Security Essentials (GSEC)
- GIAC Certified Incident Handler (GCIH)
- GIAC Security Leadership Certification

EC-Council Certifications

- CEH (Certified Ethical Hacker)
- CCISO (Certified Chief Information Security Officer)

CompTIA Certifications

- Security+
- CASP (Advanced Security Practitioner)

Cloud Security Certifications

- (ISC)² CCSP
- CompTIA Cloud+

Certification Costs

- Range from a few hundred to thousands of dollars.
- Costs include exams, training, and renewal fees

Advice for Information Security Professionals

- Put **business before technology**.
- Keep solutions **policy-driven**, not just tool-based.
- Be **quietly competent**—let results show your skill.
- Avoid ego; work should be invisible to end users.
- Be ready with a "**silver bullet**" (high-impact idea) when speaking to executives

EMPLOYMENT POLICIES AND PRACTICES

Job Descriptions – Must be specific, realistic, and include security roles.

Interviews should assess:

  - Technical skills
  - Ethics
  - Scenario-based responses

Background Checks – Includes criminal records, credit history, employment history.

Employment Contracts may include:

  - Noncompete clauses (NCCs)
  - Nondisclosure agreements (NDAs)
  - "Garden leave" (paid suspension before job switch)

New Hire Orientation – Introduce policies, systems, and expected behavior.

On-the-Job Security Training

  - Part of the SETA program.
  - Includes phishing, safe browsing, password hygiene.

Evaluating Performance – Security-related responsibilities included in evaluations.

Termination Procedures

  - Immediate access revocation
  - Collection of devices, keys, and credentials
  - Differentiated handling for **friendly vs. hostile exits**

PERSONNEL CONTROL STRATEGIES

- **Separation of duties**: Tasks require multiple people.
- **Two-person control**: Two people review each other's work.
- **Job/Task Rotation**: Prevents overdependence on one person.
- **Least privilege**: Minimal access for job function.
- **Need to know**: Access only to necessary data

Privacy and the Security of Personnel Data

- Personal data includes:
  - Names, addresses
  - SSNs, medical info, family info
- Treated as **critical data**, like trade secrets or IP.
- Must follow privacy laws and best practices

Security Considerations for Temporary Employees, Consultants, and Other Workers

Temporary Employees

- Employed via agencies; often lack contractual obligations.
- Risks:
  - Broad access to info
  - Limited accountability
- Mitigation:
  - Limit access
  - NDAs (if allowed)
  - Clean desk policies

Contract Employees

- Examples: maintenance, repair techs.
- Require **escort and scheduling protocols**.
- Security staff must confirm legitimacy.

Consultants

- Must be prescreened, contracted carefully.
- Often want to share experiences—include NDAs in contracts.

Business Partners

- Partnerships must define:
  - What data is shared
  - Format, frequency, permissions
  - Risk acceptance and legal terms

MODULE 8: SECURITY TECHNOLOGY – ACCESS CONTROLS, FIREWALLS, AND VPNS

INTRODUCTION TO ACCESS CONTROLS

- **Access control** determines how subjects (users/processes) interact with objects (files/devices).
- Goals: Confidentiality, integrity, availability.
- Four fundamental functions:
  1. **Identification** – Claiming an identity (e.g., username).
  2. **Authentication** – Verifying identity (e.g., password, biometrics).
  3. **Authorization** – Granting access based on policies.
  4. **Accountability** – Monitoring and recording activity (e.g., logs).

Access Control Mechanisms

- **Discretionary Access Control (DAC)**: Controlled by owner. Common in desktop OS.
- **Mandatory Access Control (MAC)**: Access based on security labels. Strict and centrally enforced.
- **Nondiscretionary Access Control**:
  - **Role-Based Access Control (RBAC)**: Access tied to job role.
  - **Task-Based Access Control (TBAC)**: More specific; access tied to temporary tasks.
- **Lattice-Based Access Control**: Uses levels (e.g., Top Secret, Confidential)

Biometrics

- Uses **physical or behavioral traits** for identification.
- Examples: fingerprints, facial recognition, iris scans.
- Advantages: Hard to duplicate.
- Disadvantages: Cost, privacy concerns, false acceptance/rejection.

Access Control Architecture Models

- **Trusted Computing Base (TCB)**: Security-relevant portions of a system.
- **TCSEC (Orange Book)**, **ITSEC**, and **Common Criteria**: Evaluation standards.
- **Bell-LaPadula Model**: Enforces confidentiality (no read up, no write down).
- **Biba Model**: Focuses on integrity (no write up, no read down)

FIREWALL TECHNOLOGIES

Firewall: Prevents unauthorized data transfer between trusted and untrusted networks.

Processing Modes

1. **Packet Filtering**:
   - Inspects headers (IP, port, protocol).
   - Types:
     - **Static filtering**: Fixed rule set.
     - **Dynamic filtering**: Adapts to network state.
     - **Stateful Packet Inspection (SPI)**: Tracks connection states.
2. **Application Layer Proxy Firewalls**:
   - Intercept traffic at application level.
   - Slower but more secure.
3. **MAC Layer Firewalls** – Operate at data link layer (Layer 2).
4. **Hybrid Firewalls** – Combine multiple methods.

Firewall Architectures

1. **Packet Filtering Router**: Screens traffic based on IP and ports.
2. **Dual-Homed Host**: Two NICs – one public, one private.
3. **Screened Host**: Router and bastion host combo.
4. **Screened Subnet (DMZ)**: Adds isolated buffer zone (DMZ) between internal and external networks

Selecting the Right Firewall

- Consider:
  - Business needs
  - Security policy
  - Scalability
  - Cost
  - Support & vendor reputation

Configuring and Managing Firewalls

- Use **rule bases** or **Access Control Lists (ACLs)** to define allowed/denied traffic.
- Best practices:
  - Least privilege
  - Deny by default
  - Regular log reviews
  - Documented rule changes

Content Filters

- Block unwanted or dangerous content.
- Positioned at:
  - Gateway
  - Email server
  - Endpoint
- Examples: Spam filters, URL filters, keyword scanners.

PROTECTING REMOTE CONNECTIONS

Remote Access

- Methods
  - Dial-up (rare)
  - VPNs
  - SSH
  - RDP
- Risks
  - Weak passwords
  - Unpatched endpoints
- Use **two-factor authentication** and logging.

Authentication Protocols

- **RADIUS**: Centralized AAA protocol (Authentication, Authorization, Accounting).
- **TACACS+**: Similar to RADIUS but more flexible.
- **Kerberos**: Ticket-based, time-sensitive protocol.

Virtual Private Networks (VPNs)

- Extends private networks over public infrastructure using encrypted tunnels.
- Key Components:
  - **Encapsulation**
  - **Encryption**

- **Authentication**

Types of VPNs:

1. **Trusted VPN** – Uses leased lines; trust provider.
2. **Secure VPN** – Encrypts via IPSec or SSL.
3. **Hybrid VPN** – Mix of both trusted and secure VPNs.

Tunneling Protocols

- **IPSec**:
  - **Transport mode**: Encrypts data, not headers.
  - **Tunnel mode**: Encrypts both headers and data.
- **L2TP**: Layer 2 protocol, often combined with IPSec.
- **SSL VPNs**: Uses browser-based access.

FINAL THOUGHTS ON REMOTE ACCESS AND ACCESS CONTROLS

Deperimeterization

- Concept that the traditional network boundary is fading.
- Cloud, mobile, and IoT require **zero trust** models.
- Emphasizes securing data **regardless of location**.

Remote Access in the Age of COVID-19

- Pandemic highlighted the need for resilient, scalable, and secure remote work solutions.
- VPN demand surged; unprepared orgs scrambled to scale remote access infrastructure.

MODULE 9: INTRUSION DETECTION AND PREVENTION SYSTEMS AND OTHER SECURITY TOOLS

INTRODUCTION TO INTRUSION DETECTION AND PREVENTION SYSTEMS

- IDPSs (Intrusion Detection and Prevention Systems) are designed to detect, prevent, and respond to intrusions or violations of an organization's information systems.
- An **intrusion** is any attempt to compromise the confidentiality, integrity, or availability of information systems.
- **Intrusion prevention** includes proactive measures: good security policy, training, security tech (like IDPS), and awareness campaigns.

IDPS Terminology

- **False positive**: Legitimate activity misidentified as malicious.
- **False negative**: Malicious activity not detected.
- **Alert clustering** and **correlation**: Grouping related alerts to simplify analysis.
- **Alarm filtering**: Discards low-risk alerts.

Why Use an IDPS?

- Detects known and unknown attacks.
- Logs malicious activity.
- Can take **automated action** (e.g., block IPs).
- Enforces organizational security policies.
- Helps organizations **meet compliance requirements**.

Types of IDPS

Type	Description
NIDPS (Network-Based)	Monitors network traffic, placed at strategic points like gateways
HIDPS (Host-Based)	Resides on servers or clients, monitors system calls, file access, logs
Wireless IDPS	Specialized for 802.11 wireless traffic; detects rogue access points
NBA (Network Behavior Analysis)	Detects anomalies in traffic flow: DDoS, malware, policy violations.
Hybrid IDPS	Combines multiple methods for better coverage and correlation.

IDPS Detection Methods

Method	Description
Signature-based	Detects known patterns or "signatures" of attacks (low false positives).
Anomaly-based	Compares behavior to a baseline; detects unknown attacks but more false positives.
Stateful Protocol Analysis	Examines deviations from known good protocol behaviors (e.g., FTP, HTTP).

IDPS Response Behavior

- **Passive response**: Logging, alerting, SNMP traps.
- **Active response**: Blocking IPs, resetting sessions, modifying firewall rules.
- **Trap-and-trace**: Attempts to locate source of intrusion, may raise ethical concerns.

Strengths and Limitations of IDPS

Strengths

- Real-time monitoring and alerting.
- Supports policy enforcement.
- Baseline security tracking.
- Useful for forensic investigations.

Limitations

- Cannot compensate for weak or missing security infrastructure.
- Can be overwhelmed under high load.
- Vulnerable to **false positives/negatives**.
- Complex to configure and tune.
- Can be exploited by "IDPS terrorists" who cause DoS using fake alerts.

Selecting IDPS Approaches and Products

- Evaluate based on:
  - Detection method
  - Integration with existing systems
  - Customizability and scalability
  - Vendor support and cost
- Use **NIST SP 800-94** as a guide for selecting and deploying IDPS products.

Deployment and Implementation of an IDPS

- Factors to consider:
  - Number of sensors and consoles
  - Placement (e.g., behind routers or at DMZ)
  - Data storage and analysis needs
  - Integration with SIEMs (Security Information and Event Management systems)

Measuring Effectiveness

- Use realistic test scenarios (simulate DoS, probe attacks).
- Perform **baseline assessments** before implementation.
- Continue periodic reviews.

HONEYPOTS, HONEYNETS, AND PADDED CELL SYSTEMS

Tool	Function
Honeypots	Decoy systems that attract attackers to distract them from critical assets.
Honeynets	A network of honeypots.
Padded cell	A more secure honeypot that confines the attacker in a monitored, simulated environment.

Benefits

- Learn attacker behaviors.
- Test defenses.
- Reduce risk to real systems.

SCANNING AND ANALYSIS TOOLS

Tool Type	Description
Port Scanners	Discover open ports and services (e.g., Nmap).
Firewall Analysis Tools	Identify misconfigurations or rules conflicts.
OS Detection Tools	Identify system versions and vulnerabilities.
Vulnerability Scanners	Detect unpatched systems, missing security measures (e.g., Nessus).
Packet Sniffers	Capture packets for traffic analysis (e.g., Wireshark).
Wireless Security Tools	Tools like Aircrack, Kismet, NetStumbler for detecting rogue APs and sniffing wireless traffic.

MODULE 10: CRYPTOGRAPHY

INTRODUCTION TO CRYPTOGRAPHY

- **Cryptography**: the practice of using codes to secure information.
- **Cryptanalysis**: the process of breaking cryptographic systems.
- The science combining both is called **cryptology**.
- Everyday examples: encrypted email, banking, digital signatures.

The History of Cryptology

Year	Event
1900 B.C.	Egyptians used cryptic hieroglyphs.
50 B.C.	Caesar Cipher used letter-shifting.
1466	Alberti developed polyalphabetic ciphers.
1914–17	WWI radio ciphers sparked modern cryptanalysis.
1939–42	Allies broke **Enigma**, impacting WWII.
1976	Diffie and Hellman introduced public-key encryption.
1977	RSA algorithm was created by Rivest, Shamir, Adleman

Key Cryptology Terms

- **Plaintext**: readable data.
- **Ciphertext**: encrypted data.
- **Algorithm**: mathematical rule for encryption.
- **Key**: a value used to control the encryption process.
- **Cipher**: the method of encryption.
- **Work factor**: effort needed to break encryption.

ENCRYPTION METHODS

1. **Bit Stream Cipher**: Encrypts data bit-by-bit using XOR (e.g., in stream-based algorithms).
2. **Block Cipher**: Encrypts data in chunks (e.g., 64-bit blocks).

Substitution Cipher

- Replaces characters in the alphabet.
- **Monoalphabetic**: uses one cipher alphabet.
- **Polyalphabetic**: uses multiple cipher alphabets for added security.

Transposition Cipher

- Rearranges characters of plaintext without changing them.
- Used in **rail fence cipher**, matrix ciphers, etc.

Exclusive OR (XOR)

- Combines bits where:
  - 1 XOR 1 = 0, 0 XOR 0 = 0
  - 1 XOR 0 = 1
- Used in bit stream ciphers for mixing plaintext and key bits.

Vernam Cipher

- Also called **one-time pad**.
- Uses a truly random key as long as the message.
- Unbreakable if used correctly, but hard to implement securely.

Book-based Cipher

- Uses positions of words in a shared book as keys.
- Examples include the **Beale Ciphers**.

Hash Functions

- One-way transformations of data.
- Generates a fixed-length message digest (e.g., SHA-256).
- Used in:
  - Integrity checking
  - Password storage
  - Digital signatures.

CRYPTOGRAPHIC ALGORITHMS

Symmetric Encryption

- One key for encryption and decryption.
- Examples:
  - **AES**, **DES**, **3DES**
- Fast and efficient but requires secure key distribution.

Asymmetric Encryption

- Public/private key pair.
- Examples:
  - **RSA**, **Diffie-Hellman**, **ECC**
- Supports digital signatures and secure key exchange

Encryption Key Size

- Longer keys = stronger encryption.
- 128, 192, 256 bits are common in **AES**.
- **RSA** keys range from 1024 to 4096 bits.

CRYPTOGRAPHIC TOOLS

Public Key Infrastructure (PKI)

- Includes:
  - Digital certificates
  - Certificate authorities (CAs)
  - Registration authorities
- Ensures **trust and identity** in secure transactions.

Digital Signatures

- Confirms data origin and integrity.
- Uses sender's private key to sign; receiver verifies with public key.

Digital Certificates

- Issued by CAs.
- Binds identity with a public key.

Hybrid Cryptography Systems

- Combine symmetric + asymmetric.
- E.g., RSA used to send AES session keys securely.

Steganography

- Hides data within media (images, audio, documents).
- Not encryption but obscures the existence of a message.
- Modern uses include watermarking, covert communication.

PROTOCOLS FOR SECURE COMMUNICATIONS

Protocol	Purpose
SSL/TLS	Secures websites and online sessions (HTTPS).
IPSec	Encrypts data over IP networks.
PGP	Email encryption (hybrid).
S/MIME	Secures email contents and attachments.
PEM	Email encryption using public key.
SET	Secures credit card transactions online .

Wireless Encryption

- **WEP**: Weak and deprecated.
- **WPA/WPA2**: Stronger; WPA3 is the newest standard.
- **Bluetooth**: Short range but vulnerable; use secure pairing.