



# Security+

## Domain 5: Security Program Management & Oversight

SY0-701

# Brian Olliff

Defensive Engineering Instructor

---

# Topics

**Policies & Procedures**  
**Standards**  
**Laws & Regulations**  
**Governance**  
**Risk Management**  
**Vendor Risk**  
**Compliance**  
**Audits & Assessments**  
**Security Training**

# Learning Objectives

- Understand the components of effective security governance
  - + Policies, procedures, and standards
- Be able to explain processes and elements of risk management
  - + Identification, assessment and analysis, management, and reporting
- Understand how to properly manage risk with third-party vendors
- Understand security compliance and consequences of non-compliance
- Be able to explain various types of audits and assessments
- Understand different types of security awareness programs
  - + Phishing campaigns
  - + User training and awareness

# Policies



# Policies

---

- Framework for operations, behaviors, compliance rules, etc
  - Help establish effective governance
  - Ensure organizational compliance
- Governance
  - Processes used to direct organization, expressed as policies
- Compliance
  - Adhering to regulations, standards, policies, laws
  - Policies define rules for maintaining compliance
- Guidelines
  - Recommendations instead of rules
  - More flexible than policies
  - Allow discretion in interpretation

# Common Policies

---

- Acceptable Use Policy (AUP)
  - Defines what employees may/may not do on/with company systems
    - Web browsing, email, downloads, personal use
  - Goal - ensure users do not harm organization or resources
  - Included information
    - Consequences for noncompliance
    - Details on how compliance is monitored
    - Requirement for employees to acknowledge acceptance
- Information Security Policies
  - Ensure all IT users comply with rules and guidelines
  - Focus on security of organization's systems and data

## Common Policies

---

- Business Continuity (BC) & Continuity of Operations Plans (COOP)
  - Details critical business processes that must stay operational
  - Focuses specifically on operations during disruptions or disasters
- Disaster Recovery (DR)
  - Details of steps to recover from catastrophic event
  - Major hardware failure, natural disaster, security breach, etc
  - Focus on quick & efficient restoration of systems
- Incident Response (IR)
  - Processes and steps to follow during security event/breach
  - Identification, investigation, control, mitigate



## Common Policies

---

- Software Development Lifecycle (SDLC)
  - Structured plan to detail stages of software development
  - Requirement analysis through post-deployment maintenance
- Change Management
  - How changes to systems and software are performed
  - Request, review, approval and implementation
  - Includes requirements for documentation

# Procedures



# Personnel Management

---

- Policies & procedures related to identity and access management
- Cooperation between IT and HR
- Recruitment (hiring)
  - Locating and selecting employees for various job roles
  - Requires proper screening and background checks
    - Verification of individual, no concealed criminal activity
    - May check financial, personal connections, etc
- Operation (working)
  - Policy and training communication to employees as needed
  - Often different training from different departments
- Separation (termination - firing/retire)
  - Requires collecting assets, proper offboarding procedures

## Onboarding & Offboarding

---

- Onboarding begins with HR bringing in new employees
- All new employees require access to resources
  - Workstation, accounts, email, phone, etc
- Integration with IT and HR can make process more efficient/secure
  - Account creation, secure transmission of credentials
  - Asset assignment (workstation, phone, etc)
- Includes proper training, security awareness, etc.
- Offboarding - decommission access in timely manner after leaving
  - Account disabled & privileges removed
  - Assets returned, data on personal devices removed
    - Mobile devices, keys (physical/security), smart cards, USB media, etc

# Playbooks

---

- Checklist of items designed to follow a specific workflow
  - Standard operating procedure
  - Ensures consistency, quality, and effectiveness
- Assist with sharing information with new employees
  - New roles, new to organization
  - Defined documentation of critical procedures
- Allows for effective monitoring and improvement of procedures
- Incident response
  - Details of emergency procedures, contingency plans
  - Help with quick decisions by responders
  - Can reduce impact of incident with effective & clear plans

# Change Management

---

- Any change requires careful planning
  - Including how the change will affect other systems & processes
- Significant changes require testing before implementation
  - Test or development environment only
- All changes should include rollback plans
- Careful scheduling for changes that may cause downtime
- Change management documentation
  - Request with steps to implement
  - Input from affected teams
  - Approval and scheduling
  - Review of change after implementation

# Standards



# Standards

---

- Define expected outcome of certain activity or task
  - Configuration of server
  - Performance baselines
- Often driven by regulatory requirements
  - Standards may vary based on industry and location
  - Ex: US healthcare - HIPAA
- Many standards built around risk management
  - Resilience against security incidents/data breaches
- Organizations often stick with accepted industry standards
- Selection of standards involves strategic planning
  - Legal/regulatory requirements, business needs, risk management, best practices



# Common Industry Standards

---

- ISO/IEC 27001 & 27002
  - International standard provides framework for security controls
  - 27002 companion that provides detailed guidance on specific controls
- ISO/IEC 27017 & 27018
  - Extensions to 27001 for cloud services/PII in cloud services
- NIST SP 800-63
  - US Govt standard for digital identities, password & access control reqs
- PCI DSS
  - Requirements for handling and protecting credit card information
- FIPS
  - Standards/guidelines developed by NIST for federal computer systems

# Passwords

---

- Technical requirements for design, implementation, & PW management
- Hashing algorithms
  - Requirements for hash functions used for password storage
- Password salting
  - Methods used to protect passwords from rainbow table attacks
- Secure transmission
  - Details for secure password transmission (including specific cipher suites)
- Password resets
  - Requirements for appropriate identify verification
- Password managers
  - Org approved options (or lack of option), requirements for storage

# Access Control

---

- Ensure only authorized users can access data/systems
- Access control models
  - Which models can be used in different situations (RBAC, MAC, DAC, etc)
- Identity verification
  - Acceptable methods to verify users (passwords, tokens, biometric, etc)
- Privilege management
  - How least-privilege access is implemented and enforced
- Authentication protocols
  - Acceptable authentication protocols - Kerberos, OAuth, SAML
- Session management
  - Requirements for session timeouts, secure cookie usage, etc
- Audit trails
  - Mandatory auditing requirements

# Physical Security

---

- Protection of wiring closets, datacenters, cabling, hardware, etc
- Building security
  - Card access systems, CCTV, security personnel
- Workstation security
  - Physically securing desktop computers and laptops
- Datacenter/server room security
  - Card access requirements, biometric, sign-in/out logs, escorted access
- Equipment disposal
  - Requirements to securely retire/repurpose equipment to protect data
- Visitors
  - Requirements for any non-employee, sign-in/out, badges, escort reqs

# Encryption

---

- Protecting data from unauthorized access
  - At rest & in transit
- Encryption algorithms
  - Acceptable algorithms that can be used for protection
- Key length
  - Minimum length for each allowed type of encryption
- Key management
  - How keys are generated, distributed, stored, changed, and revoked
  - Often requires use of secure key management system (KMS)

# Laws and Regulations



## Legal Considerations

---

- Multiple regulations and laws must be considered in security
- Vary based on industry and location
- Governance teams/committees must manage
  - Compliance requirements
  - Contractual obligations & license agreements
  - Public disclosure & breach notification laws
  - Privacy laws
- Several frameworks and benchmarks exist to assist
- Due diligence required
  - Responsible parties have done everything they can
  - Without being negligent in duties

# Global Laws

---

- Many locations have enacted wide reaching laws
- General Data Protection Regulation (GDPR)
  - Personal data can't be collected, processed, stored without informed consent
    - Some legal & public interest exceptions
    - Data only collected/processed for stated purpose, clearly described
  - Right to withdraw consent, inspect or erase data
- California Consumer Privacy Act (CCPA)
  - California residents - right to know what personal information is collected
    - Purpose of collection, and where data shared
  - Right to access data, delete, or opt out of sale
  - Organizations must inform about categories of data collected
  - Applies to any organization that provides goods or services to CA residents



## National, Regional & Industry Laws

---

- Countries/regions have laws that apply to various industries
  - US and EU healthcare (HIPAA and GDPR)
  - US and Canada energy sector (NERC)
  - US and UK government (FISMA, CJIS, GSC)
- Most cybersecurity laws have national/international scope
  - Result of global nature of internet
- Other laws are more regional or local
  - States, provinces, territories, cities, etc
- Important to understand what applies to specific organization
  - Based on location, industry, customers, etc

# Governance



# Governance

---

- Practices to ensure organizations follow regulations and laws
- Designed to protect from legal liability
- Oversight on multiple legal risks
  - Regulatory requirements, contract obligations, public disclosure laws
  - Breach liability, privacy laws, IP protection, licensing requirements
- Policies require constant updates and revisions
  - Monitoring of changes in legislation that apply
  - Audits & inspections of policies, procedures, standards to ensure compliance
  - Results from audit and new requirements drive revisions
  - Updates may require additional employee training

# Governance Structures

---

- Governance boards
  - Senior executives and external stakeholders
  - Responsible for ensuring compliance
  - Set objectives, policies, and guidelines for security and risk management
  - Ensure security is a top strategic priority
- Governance committees
  - Subject matter experts and department/team representatives
  - Provide analysis, recommendations, and operational support
  - Focus more on specific issues, instead of broad strategies

# Centralized and Decentralized Governance

---

- Centralized
  - Single core group/department primarily responsible
  - Establish policies, procedures, guidelines for organization
  - Personnel and budget (for compliance) controlled by single group
- Decentralized
  - Multiple groups/departments assume responsibility
  - Decisions based more on local needs and priorities
  - Different teams have more granular control over resources
- Choice depends on organization size, structure, & risk appetite

## Government Entities

---

- Governmental governance committees based on country/jurisdiction
- Regulatory agencies
  - Establish/enforce standards, guidelines, regulations for different industries
- Intelligence agencies
  - Gather and analyze information to ID potential threats
  - Provide information to government groups
- Law enforcement - enforce laws and regulations
- Defense/military organizations
  - Safeguard national security, protect country from external threats
- Data protection authorities
  - Protection of personal data and privacy rights, enforce data protection regulations
- National cybersecurity agencies
  - Protect critical infrastructure, govt networks, other national interests

# Data Governance

---

- Relies on various roles to maintain security oversight and control
  - Specialized and independent roles, with unique responsibilities
  - Coordination between roles is critical
- Owner
  - Director/VP role, responsible for ensuring data is protected
  - Identifies classification/sensitivity, who accesses, and what level of security
- Controller
  - Individual, public authority, agency, ect
  - Identifies purposes, conditions, means of processing personal data
  - Ensures data processing adheres to all legal requirements

# Data Governance

---

- Processor
  - Responsible for processing data on behalf of controller
  - Cloud service provider, vendor, or business partner
  - Must keep records of all data activities
  - Ensures data handled securely, according to rules from owner & controller
- Custodian
  - Also called data steward - often IT department
  - Responsible for safe storage & transport of data
  - Implements & enforces all security controls established by owner/controller
  - Reports any issues that may indicate security incident



# **Risk Identification & Assessment**



# Risk Identification

---

- First step in any risk assessment/analysis process
  - Allows decisions about resources, mitigation strategies, & risk management
- Technical risks
  - Malware attacks, phishing attempts, hardware failure, vulnerabilities
- Non-technical risks
  - Inadequate policies, lacking training
- Multiple methods to identify
  - Vulnerability assessments, penetration testing
  - Security audits
  - Threat intelligence

# Risk Assessment

---

- Evaluation of identified risks to determine potential impact
- Ad-hoc
  - Assessment conducted as needed, in response to specific event
- One-time
  - Comprehensive evaluation, normally during initial system deployment
  - Also performed when independent assessment is needed
- Recurring
  - Scheduled at regular intervals (monthly, quarterly, annually)
  - Audits, compliance checks, vuln scans, etc
- Continuous
  - Constant evaluation of risks, usually with specialized tools
  - Agent-based vuln scans, IDS reports, etc

# Risk Analysis



# Risk Analysis

---

- Risk analysis
  - Process of identifying and evaluating potential risks
  - Evaluate nature of risks, their causes, consequences and concerns
- Risk assessment
  - Systematic approach of estimating risk levels and significance
- Likelihood - probability of any given threat occurring
  - Used in qualitative analysis (low, medium, high or numeric scale)
- Impact - severity of risk if occurs
  - Can be determined by value of asset, cost of disruption, etc.
- Probability - quantitative measure
  - Precise measurement of chance of risk based on statistics
- Inherent risk - level of risk before any mitigation attempted
  - Result of risk analysis

# Quantitative Risk Analysis

---

- Assigns specific values to risk factors
- Exposure factor (EF)
  - Percentage of the asset value that would be lost
- Annualized rate of occurrence (ARO)
  - Number of times loss is expected per year
- Single loss expectancy (SLE)
  - Amount lost in a single occurrence of risk factor
  - Value of asset multiplied by exposure factor
- Annualized loss expectancy (ALE) - amount lost over 1 year
  - SLE multiplied by ARO
- Values do not refer to only monetary or material value

# Qualitative Risk Analysis

---

- Assessment based on subjective judgement instead of precise numbers
  - Focuses mainly on identifying risk factors
- More accessible method
  - Simpler and often faster analysis
- Identifies risks by considering causes, consequences, & impacts
- Some limitations compared to quantitative
  - Subjective - relies on judgement of individuals
  - Can introduce bias & inconsistency if opinions differ
  - Can make presenting information more difficult without concrete numbers
- Even with limitations, still important
  - Ability to quickly draw attention to important/significant risks

# Risk Register

---

- Document that shows results of risk assessment
- Heat map risk matrix - graph indicating likelihood and impact of risk factors
  - Impact & likelihood ratings, date ID'd, status
  - Description & possible countermeasures
  - Escalation route
- Scatterplot graph
  - Impact & likelihood each an axis
  - Associated plot point includes information about nature of risk
- Should be shared with stakeholders to understand associated risks
- Risk threshold
  - Levels of acceptable risk org can tolerate



## Key Risk Indicators (KRIs)

---

- Predictive indicators, used to monitor and predict potential risk
  - Help provide early indication of increasing risk exposure
  - Combine potential impact/likelihood for leadership to take proactive steps
- Risk owner - individual responsible for specific risk
  - Identification, assessment, mitigation, monitoring, etc.
- Risk appetite - level of risk organization is willing to accept
  - Helps determine risks to add to risk register, and priority
  - Three levels - expansionary, conservative, neutral
- Risk tolerance
  - Accepted org tolerance between measured risk level and risk appetite
  - If risk potential impact/likelihood > risk tolerance, add to risk register

# Risk Management



# Managing Risk

---

- **Risk cannot be eliminated**
- Goal is to mitigate risk factors to acceptable level for organization
- Risk mitigation/remediation
  - Process of reducing exposure to the effects of risk factors
- Risk deterrence/reduction
  - Countermeasure that reduces exposure to threat
- Multiple strategies exist for how to handle inherent risk
  - Level of risk before any mitigation/countermeasures attempted

# Risk Management Process

---

- Identify critical business functions
  - Any functions or processes that support business operations
- Identify vulnerabilities
  - Analysis of systems/assets that support critical workflows/functions
  - Discovery of weaknesses or vulnerabilities (not just technical)
- Identify threats
  - Identify threat source, possible actors that could exploit vulnerabilities
- Analyze business impacts
  - Quantitative and qualitative analysis methods
- Identify risk response
  - Identify countermeasures & cost of deployment
  - Other risk responses as needed

## Accept Risk

---

- No countermeasures put in place, no patches applied, etc
  - Level of risk does not justify action
- Risk exception
  - Risk cannot be mitigated using standard practices/within specified time
  - Financial, operational, technical reasons
  - Risk recognized, seeking other mitigation methods
  - Should only be temporary
- Risk exemption
  - Risk can remain without being mitigated
  - Intentional business decision
  - Often because cost of mitigation higher than potential damage

# Transfer Risk

---

- Also known as risk “sharing”
- Assigning (transferring) the risk to a third-party
  - Typically through an insurance company (cybersecurity insurance)
  - Contract with vendor who accepts some liability
- Normally only financial risk/liability is transferred
- Some risk cannot be transferred or shared
  - Risk to reputation after incident
  - Legal liability (situation dependent)
- Not a reason to ignore (or accept) risk without careful consideration
  - Most transference requires some level of mitigation as well

## Avoid Risk

---

- Stopping whatever activity that is creating the risk
  - Results in eliminating specific risk (usually temporarily)
- Example:
  - Application running on server has a critical vulnerability
  - No patch is currently available, application is not mission critical
  - Shut down server until patch is available
- Many different ways to avoid risks
  - Some can be permanent, depending on situation
  - Most are temporary and will need some further mitigation eventually

## Mitigate Risk

---

- Reducing exposure to the effects of risk factors
- Taking some action to reduce risk, while still maintaining operations
- Maintaining up-to-date software
- Deploying controls and countermeasures to detect & reduce threats
  - EDR, network firewall, data encryption, etc
  - Intended to make risk incident less likely, or reduce the cost of incident



# Business Impact Analysis



# Business Impact Analysis (BIA)

---

- Assessment of what losses might occur in various scenarios
  - Financial
  - Operational (business processes)
  - Reputational
- Example: If attacker took down public website for 8 hours
  - Quantify losses from customers not being able to place orders
  - Identify potential lost business from new customers going elsewhere
    - Also existing customers stopping businesses
  - Identify amount of time to repair & bring site back online
- Uses combination of historical data and projections for analysis

# Identify Critical Business Components

---

- Critical system identification
  - First step in any assessment or analysis
- Inventory of business processes and supporting assets
  - People, physical assets, intangible assets, procedures
- Dependency identification through business process analysis (BPA)
  - Analysis performed to help reduce interdependency between components
  - Inputs, hardware, staff, outputs, process flow
- Mission essential functions (MEF)
  - Business processes/functions that cannot be delayed
  - Analysis using four metrics

# MEF Metrics

---

- Maximum tolerable downtime (MTD)
  - Longest time function can be interrupted before unrecoverable business failure
- Recovery time objective (RTO)
  - Period of time after an incident that a system may remain offline
  - Total time to identify, troubleshoot, and recover/restore
- Work recovery time (WRT)
  - After system recovery, additional time needed to fully support function
- Recovery point objective (RPO)
  - Amount of data loss a system can sustain (measured in time)
  - When recovering data/system, recovery point is no older than RPO indicates

# Reliability Measurements

---

- Mean time between failures (MTBF)
  - Expected lifetime of product
  - Total operational time divided by number of failures
  - 100 servers, run for 1,250 hours, 4 fail = MTBF is 31,250 hours/failure
- Mean time to repair (MTTR)
  - Amount of time taken to restore system to full operation
  - Total number of hours of unplanned maintenance, divided by # of failures
  - Average value used to estimate if RTO is achievable
- Higher MTBF shows greater reliability and longer time between failures
- Lower MTTR shows faster recovery/restoration

# Vendor Selection & Assessment



# Vendors

---

- Any external person/org that provides services, goods, etc to org
- Selection involves multiple steps
  - Identifying risk criteria
  - Due diligence - using best practice/reasonable care when selecting
  - Selecting vendor based on risk profile
- Assessment is critical part of selection process
  - Evaluation of capabilities, practices, security measures
  - Frequently required for compliance reasons
  - Provide evidence of due diligence and compliance checks
- Avoid conflict of interest

# Conflict of Interest

---

- Competing interest or obligation that may compromise relationship
  - Ability to act objectively, impartially, or in best interest of other party
- Identify any potential conflicts
  - Financial
    - Partnerships, commissions, financial biases
  - Personal relationships
    - Ties with decision makers
  - Competitive relationships
    - Business relationship or competitive interest with other vendor
  - Insider information
    - Access to confidential info about other org/vendor plans



## Assessment Methods

---

- Thorough investigation and evaluation
  - Exercising due diligence in selection process
  - Uncover undisclosed risks/issues & understand capabilities/limitations
- Penetration testing
  - Test vendor's infrastructure or receive reports on recent test
  - Gain insight on possible vulnerabilities that attackers could exploit
- Right-to-audit clause
  - Provision in contract that allows org to conduct audits/assessments
  - Operational practices, IT systems, security controls, etc
  - Helps to identify deficiencies, compliance issues, security standards

## Assessment Methods

---

- Evidence of internal audits
  - Checking for independent, objective evaluation of controls & practices
  - Presence, effectiveness, and frequency of internal audits
- Independent assessments
  - Third-party audits to verify security, compliance, other capabilities
  - Provide objective, unbiased look at vendor operations
- Supply chain analysis
  - Vendors are essential part of supply chains, each with own capabilities/risks
  - Evaluation of risks/vulnerabilities associated with vendors' partners
  - Can help identify weak links
- Continuous monitoring and evaluation, regardless of method
  - Regular reviews, assessments, real-time monitoring of activities

# Vendor Agreements



# Initial Agreements

---

- Govern overall relationship with vendor, based on services provided
- Memorandum of Understanding (MOU)
  - Non-binding agreement, first step before more formal agreement(s)
  - Outlines goals and general terms of cooperation
- Memorandum of Agreement (MOA)
  - Formal, legally binding agreement
  - Outlines terms, conditions, responsibilities
  - Establishes objectives, resources, roles and obligations
- Nondisclosure Agreement (NDA)
  - Legally binding agreement, usually signed with MOA
  - Ensures confidentiality of sensitive information

# Initial Agreements

---

- Business Partnership Agreement (BPA)
  - Long-term partnership between organizations
  - Usually includes goals, financial agreements, IP rights, dispute resolution
- Master Service Agreement (MSA)
  - Overall terms and conditions for a specific contract
    - Can be for specific engagement, or overall agreement
  - Includes scope, prices, deliverables, and IP rights

## Detailed Agreements

---

- Specify more detailed operational terms for engagements
- Service-level agreement (SLA)
  - Defines metrics and standards expected from vendor
  - Often includes specific service level details
- Statement of work (SOW) (or work order/WO)
  - Details a specific project or engagement
  - Scope, deliverables, timelines, responsibilities, etc
- Questionnaires
  - Information about vendors' security practices, controls, risk management
  - May ask specific information about industry-specific regulations/standards
  - Details about security training for employees, third-party assessments
  - Answers should be supported by documentation or evidence

# Rules of Engagement (RoE)

---

- Define parameters and expectations
  - Responsibilities, communication methods, reporting, security, compliance, etc
  - Clear guidelines for vendor (behavior, activities, access to systems, etc)
- Rules should contain standard elements
  - Roles and responsibilities
  - Security requirements
  - Compliance obligations
  - Reporting and communication
  - Change management
  - Contractual provisions

# Compliance Monitoring & Reporting





# Monitoring

---

- Helps ensure organization is adhering to legal/regulatory requirements
  - Internal practices and policies
  - Assessment of third-party vendors & business partners
- Attestation and acknowledgement both required
  - Formal recognition and commitment to obligations
- Performed internally, and by third-parties
  - Self-assessments, internal audits and reviews
  - External regulatory assessments
- Automation with compliance management software
  - Assists with data collection, analysis, and reporting
  - Streamlines activities and improves accuracy
- Coupled with reporting to provide evidence of compliance

# Reporting

---

- Provides proof of compliance with laws and regulations
- Both internal and external reporting are required
- Internal
  - Primarily for internal stakeholders
  - Risk managers, senior leadership, security analysis, privacy officers
  - Focus more on operational details
- External
  - Targets external stakeholders
  - Shareholders, customers, vendors/business partners, regulators
  - High-level summaries of compliance
  - More designed to align with regulatory requirements (standardized)

# **Non-compliance Consequences**



# Data Breaches

---

- Occurs when any data/information is accessed without authorization
  - Depending on data, can have severe consequences
- Reputational damage
  - Negative publicity, loss of trust, lost customers
- Fines
  - Depending on industry/region, government fines may apply
- Theft of intellectual property
  - May result in loss of revenue, customers, etc
  - Can be difficult to remedy with legal action
- Data breaches may require notifications
  - Public, regulatory bodies, stakeholders, etc

# Non-Compliance

---

- Consequences vary by jurisdiction, industry, & regulation
- Sanctions - penalties or disciplinary actions
  - Imposed by governing bodies, regulatory authorities
- Fines from regulatory agencies
  - Vary depending on severity of violation and regulation
- Reputation harm
  - Loss of trust from customers/clients
  - Decreased business and revenue
- Non-compliance with software licenses can result in revocation
  - May also include fines or other legal actions
  - Exceeding license #s, unauthorized sharing/distribution, altering code

# Contractual Noncompliance

---

- Breach of contract
  - Failure to meet any obligations in contact may lead to legal consequences
  - Potential financial liability
- Termination of contract
  - Contracts typically include clauses allowing termination
    - Failing to protect data, insufficient security controls, etc
  - May include termination penalties
- Indemnification and liability
  - Contracts may include to shift responsibilities onto noncompliant party
- Noncompliance penalties
  - May include specific penalties for various portions of contract
  - Aim to incentivize parties to adhere to terms

# Privacy



# Data Privacy

---

- Any sensitive or personally identifiable information
  - Personal, financial, social identity, etc
  - If exposed, has potential to affect individual privacy rights
  - Type of confidential data, but specifically affects individuals
- Data subjects have right to access, correct, and request deletion of data
  - Individual identified by private data
  - Handling of this frequently requires explicit consent from data subject
- Multiple laws/regulations in place for handling private data
  - Local, regional, national, & global scopes
  - Rights of individuals, responsibility of orgs, procedures for data protection



# Private Data Ownership

---

- Ownership often not considered
- Data protection laws focus more on data subject than owner
- Organizations are considered controllers/stewards of private data
- Right to be forgotten
  - Fundamental right in GDPR
  - Grants data subjects right to request deletion under certain circumstances
  - Designed to recognize importance of individual privacy
  - Some situations where right may be limited
    - Legal requirements or claims
    - Processing needed to exercise right of freedom of expression

# Data Inventory

---

- Some laws require detailed record of data collected, processed & stored
- Data inventories provide this record
  - Type of data being handled and purpose for processing
  - Legal basis for data handling
  - Recipients of any private data
- Organizations must have lawful basis for processing personal data
- Data can only be keep as long as necessary for intended purpose
  - Or as required by law
  - Known as data retention
  - Data inventories help organizations with this requirement
    - Also assist with responding to requests for access, changes, deletion

## Legal Implications

---

- National laws enforced by data protection authorities/supervisory bodies
  - Authority to investigate breaches, issue fines, and take legal action
- Global laws/regulations
  - GDPR - General Data Protection Regulation covers all EU citizens
  - Applies to all organizations that process data of EU residents
    - Regardless of organization location
  - CCPA - California Consumer Privacy Act similar for CA residents
- Organizations have responsibility to follow laws and regulations
  - May vary by industry and geographic location
  - Some may apply based on what data is handled

# Roles and Responsibilities

---

- Data subject
  - Individual identified by personal data
  - Specific rights/protections under data protection laws (GDPR/CCPA)
  - Right to access and get information on how data used
    - Why collected, categories, data recipients, data retention periods
  - Right to request correction and deletion of personal data
- Data controller
  - Entity or org that determines how and why data is processed
  - Overall control and responsibility, including compliance and legal
- Data processor
  - Processes data on behalf of controller, no independent decision-making
  - Legal obligation to process only by controller instruction

# Audits & Assessments



# Attestation

---

- Verification and validation of security controls and processes
  - Accuracy and effectiveness
- Formal confirmation controls/practices align with standards, regulations
  - Independent, objective - performed by auditor or assessor
- Provides assurance to multiple parties that controls are effective
  - Stakeholders & management
  - Customers, vendors, & business partners
  - Regulators
- Important for organizations to perform both internal and external audits

## Internal Audits/Assessments

---

- In-depth evaluation conducted by organization's employees
- Designed to support continuous monitoring and improvement
- Compliance assessment
  - Ensure operations align with laws, regulations, policies, etc
  - Evaluate internal controls, identify non-compliance issues
- Audit committee
  - Oversight of financial reporting, internal controls, risk management practices
  - Board members, not part of org management
  - Often work with external auditors
- Self-assessment
  - Individual or organizational evaluation of performance & practices
  - Used to identify strengths and weaknesses for proactive improvement

# External Audits

---

- Performed by outside, third-party providers
  - Use specialized expertise and knowledge for impartial, objective evaluation
- Regulatory assessment
  - Typically performed by regulatory authority/agency
  - Ensures org follows mandatory regulatory requirements
  - May involve inspections, audits, review of processes, practices, & controls
  - Designed to protect public interests/customers, & uphold industry standards
- Examination
  - Independent evaluation, assesses financial statements, processes, controls
    - Checks for accuracy, reliability, and compliance
  - Focus on verifying information accuracy and compliance



# External Audits

---

- Assessment
  - Typically broad evaluation to assess overall performance and practices
    - Conducted by industry experts or consultants
  - May focus on specific areas
  - Provides objective, independent view on strengths, weaknesses, improvement areas
- Independent third-party audit
  - Focus on systems and controls, as well as processes and procedures
  - Can attest to org's focus on quality, compliance, and governance
  - Designed for stakeholder, business partner, customer confidence
    - Demonstration of transparency and accountability

# Penetration Testing



# Pen Testing

---

- Also known as ethical hacking
- Ideally designed to replicate an attack by threat actor
- Authorized engagement
  - Agreement and statement of work if performed by third-party
  - If internal, team has clear boundaries and guidelines
- More in-depth than normal vulnerability scans
  - Find vulnerabilities using various methods (scanner, fingerprinting, etc)
  - Bypass and test security controls
  - Attempt to exploit those vulnerabilities
- By definition, pen testing is intrusive testing
  - Always has possibility to cause downtime

# Reconnaissance

---

- Provides information to help testers understand targets
- Passive
  - Information gathering without direct interaction with target systems
  - Less intrusive, less chance of detection
  - OSINT (Open Source Intelligence)
  - Network traffic analysis
  - Social engineering
- Active
  - Uses tools to interact with target systems and gather information
  - May trigger alerts and notify security teams
  - Port scanning & service enumeration
  - System fingerprinting
  - DNS and web application enumeration

# Testing Methods

---

- Organization can choose based on various requirements
- Known environment
  - “Attacker” is provided information about network/attack surface
  - Useful for simulating attackers that have already breached perimeter
    - Insider threats
- Unknown environment
  - Attacker is provided with no information about attack surface
  - Requires reconnaissance prior to attack phase
  - Most closely simulates external threat actors
- Partially known environment
  - Attacker is given some information
  - Will usually require some level of reconnaissance

## Exercise Types

---

- Offensive (red team)
  - Goal is to test security controls and attempt to infiltrate system(s)
  - Identify weaknesses and potential attack vectors
- Defensive (blue team)
  - Evaluates security measures, detection, and incident response
  - Uses monitoring and alerting systems to detect and possibly prevent attacks
- Integrated (purple team)
  - Combination of offensive and defensive exercises simultaneously
  - Discuss what actions have been taken by offensive team
    - And where attempts were successful
  - Discuss what defensive team has detected and prevented
  - Red vs blue - teams do not discuss until exercises are completed

# Physical Pen Testing

---

- Assesses organization's physical security controls & practices
- Simulates real-world attacks against physical security
  - Security systems
  - Access control mechanisms
  - Surveillance
  - Perimeter defense systems
- Tester attempts to gain physical access to restricted areas
  - Social engineering
  - Lock picking
  - Tailgating
  - Bypassing alarms & surveillance systems
  - Exploiting physical vulnerabilities

# User Training





# User Training

---

- All employees need security awareness training
  - End users, executives, technical staff, etc
  - Different levels of training based on role and access levels (not titles)
  - Typically performed using computer-based training
- Overview of security policies (and penalties)
- How to identify incidents and how to report
- Security procedures for sites (guests, personal devices, secure areas)
- Data handling (PII, encryption, confidentiality, etc)
- Password and account management
- Common attack awareness (social engineering, malware, phishing, etc)
- Secure use of software - browsers, email, internet access, social sites

# Security Awareness Training Topics

---

- Policies and handbooks
  - Familiarization with policies, guidelines, acceptable use, data handling
  - Emphasis on importance of adherence to keep org safe
- Situational awareness
  - Help users to recognize/respond to potential threats
  - Vigilance, observation, prompt reporting
- Insider threat
  - Education on threat, recognition of signs
- Password management
  - Strong, unique passwords with no password reuse (general best practices)
  - Multifactor authentication

# Security Awareness Training Topics

---

- Removable media & cables
  - Risk of using unauthorized devices - theft or loss of data
  - Potential for malicious devices and charging cables
- Social engineering
  - Awareness of attack methods and vectors
  - How to avoid being a victim of social engineering (critical thinking)
  - Proper reporting
- Operational security
  - Good security practices in general day-to-day work
  - Physical & workstation security, secure comm, incident reporting
- Hybrid/remote work
  - Proper use of secure access methods, physical & data security

# Phishing Campaigns

---

- Simulated phishing attacks to educate and train
  - Signs of phishing and how to recognize
  - Proper actions to take (not clicking/responding, how to report)
- Awareness of common techniques and tactics
  - Urgent requests
  - Spoofed senders
  - Enticing offers
- Simulated campaigns provide safe method to introduce phishing
- Reporting can show user actions
  - Email opened, link/attachment clicked, message reported
- Goal is to get users to properly recognize and respond

# Recognizing Suspicious Behavior

---

- Anomalous behavior
  - Actions that significantly deviate from expectations
  - Unusual network traffic, account activity, system events, etc
- Risky behavior - actions that threaten security, systems, or network
- Unexpected behaviors
  - Any actions that deviate from established security policies
  - Occur from lack of awareness, carelessness, or malicious intent
  - Unauthorized access, bypassing controls, disregarding physical security
- Unintentional behaviors
  - Unexpected behaviors, but without malicious intent
  - Human error, lack of training, lack of understanding of policies
  - Accidental data breach, mishandling information, social engineering victim

# Training Development & Execution



# Training Lifecycle

---

- Assessment
  - What are the organization's security needs and risks?
- Planning & design
  - Objectives, topics, delivery methods of training
- Development
  - Training content created (information and materials)
- Delivery & implementation
- Evaluation & feedback
  - Assess effectiveness of training, gather insights from participants
- Ongoing reinforcement
  - Additional training to refresh information
- Monitoring & adapting

# Training Execution

---

- Training must address relevant security topics & skills
  - Effective education & instruction to enhance employee knowledge
- Engaging training and exercises
  - Clear language, avoiding excessive technical jargon
  - Real-world examples to put training in context
  - Interactive portions (quizzes, simulations, etc)
- Depending on delivery method, discussion and Q&A
- Assessments to help participants gauge level of understanding
- Feedback is important to ensure training is effective and relevant
- Regular reviews and updates on training materials
  - Best practices, new threats/attacks, updated regulations



## Reporting and Monitoring

---

- Used to gauge effectiveness of training
- Initial effectiveness - immediate impact of training on participants
  - Measures knowledge & awareness immediately after completing training
  - Pre- and post-training exercises, quizzes, or surveys
- Recurring effectiveness - long-term impact and sustainability of training
  - Measures retained knowledge in day-to-day activities
- Both are important to measure overall success of training

## Reporting & Monitoring Methods

---

- Assessments and quizzes
  - Pre- and post-training
- Incident reporting
  - Data tracked from incidents over time assess training impact incidents
- Phishing simulations
- Observations and feedback
  - Manager and supervisor feedback on employee security behaviors
- Metrics and performance indicators
  - Reported incident numbers, policy compliance, etc
- Training completion rates

*EXPERTS AT MAKING YOU AN EXPERT*

