

# CISSP® Common Body of Knowledge: Operations Security Domain

Version: 5.9.2



*CISSP Common Body of Knowledge Review* by Alfred Ouyang is licensed under the Creative Commons Attribution-NonCommercial-ShareAlike 3.0 Unported License. To view a copy of this license, visit <http://creativecommons.org/licenses/by-nc-sa/3.0/> or send a letter to Creative Commons, 444 Castro Street, Suite 900, Mountain View, California, 94041, USA.

# Operations Security Domain

---

Security Operations domain is used to identify critical information and the execution of selected measures that eliminate or reduce adversary exploitation of critical information. It includes the definition of the controls over hardware, media, and the operators with access privileges to any of these resources. Auditing and monitoring are the mechanisms, tools and facilities that permit the identification of security events and subsequent actions to identify the key elements and report the pertinent information to the appropriate individual, group, or process.

The candidate is expected to know the resources that must be protected, the privileges that must be restricted, the control mechanisms available, the potential for abuse of access, the appropriate controls, and the principles of good practice.

# Operations Security Domain

---



## Concept & Definition

- Identification of Resource Protection Needs
- Threats to Information Operations
- Security Controls & Countermeasures

# CISSP “Operations Security”

---

- CISSP Operations Security Domain focuses on information security operations.
- CISSP operations security objectives are:
  - Reduce the operational vulnerability and threats to confidentiality, integrity and availability.
  - Protect organization’s computing resources and information assets.
  - Balance:
    - Ease-of-use and system controls;
    - Value of data and business/mission needs.
  - Compliance with laws, regulations and organizational policies.

# Security Practices

---

- Need-to-know
  - Subjects should only have access to objects that enables them to perform their assigned job functions.
- Least privilege
  - Subjects should only have sufficient access privilege that allows them to perform their assigned work.
- Separation of duties
  - No single person should be responsible for approving his/her own work.
- Job rotation
  - To reduce risk of collusion and to ensure no single point of failure.
- Mandatory vacation
  - To allow auditors to review records.

# Categories of Security Controls

---

- Management (Administrative) Controls
  - Policies, Standards, Processes, Procedures, & Guidelines.
    - Administrative Entities: Executive-Level, Mid.-Level Management.
- Operational (and Physical) Controls
  - Operational Security (Execution of Policies, Standards & Process, Education & Awareness).
    - Service Providers: InfoSec/IA Department, Program Security, Personnel Security, Document Controls (or CM), HR, Finance, etc.
  - Physical Security (Facility or Infrastructure Protection)
    - Locks, Doors, Walls, Fence, Curtain, etc.
    - Service Providers: Facility Security Department, Guards, Dogs.
- Technical (Logical) Controls
  - Access Controls , Identification & Authentication, Authorization, Confidentiality, Integrity, Availability, Non-Repudiation.
    - Service Providers: Enterprise Architect, Security Engineer, CERT, SOC, NOSC, Helpdesk.

# Types of Security Controls

---

- **Directive controls**: Often called administrative controls, these are intended to advise employees of the behavior expected of them during their interfaces with or use the organization's information systems.
- **Preventive controls**: Included in preventive controls are physical, administrative, and technical measures intended to preclude actions violating policy or increasing risk to system resources.
- **Deterrent controls**: Deterrent controls involve the use of warnings of consequences to security violations.
- **Detective controls**: Detective controls involve the use of practices, processes, and tools that identify and possibly react to security violations.
- **Corrective controls**: Corrective controls also involve physical, administrative, and technical measures designed to react to detection of an incident in order to reduce or eliminate the opportunity for the unwanted event to recur.
- **Recovery controls**: Once an incident occurs that results in the compromise of integrity or availability, the implementation of recovery controls is necessary to restore the system or operation to a normal operating state.

# Due Care vs. Due Diligence

---

- Due Care:
  - Policies and implemented actions that an organization has taken to minimize risk to its tangible and intangible assets (e.g. information assets, customers, employees, and resources.)
  - Example: Installation of anti-virus (AV) system
- Due Diligence:
  - Continual actions that an organization are doing to protect and minimize risk to its tangible and intangible assets.
  - Example: Keeping virus signatures up to date



## Questions:

---

- Personnel security policy, procedure, and guidelines are what type of operational security control?  
—
- Communicating security policy, conducting annual security awareness training, and exercise business continuity planning (BCP) are what type of operational security control?  
—
- Performing periodic background re-investigation is what type of operational security control?  
—

## Answers:

---

- Personnel security policy, procedure, and guidelines are what type of operational security control?
  - Directive (or Administrative)
- Communicating security policy, conducting annual security awareness training, and exercise business continuity planning (BCP) are what type of operational security control?
  - Preventive
- Performing periodic background re-investigation is what type of operational security control?
  - Detective

# Operations Security Domain

---

- Concept & Definition
- ➔ Identification of Resource Protection Needs
- Threats to Information Operations
- Security Controls & Countermeasures

# Identification of Resource Protection Needs

---

- Information is an organizational asset
  - Information classification
    - Identify information assets
    - Identify IT assets that store, process, and transmit data
    - Define protection level
  - Define security objectives
    - Confidentiality, integrity, and availability (i.e., FIPS 199)
- Protection of information assets is a “system” that consists of:
  - People (i.e., management and operational controls)
  - Process (i.e., management and operational controls)
  - Technology (i.e., technical controls)

## Protection of Information ...<sup>(1/2)</sup>

---

- Level of protection is determined by sensitivity of information assets
- Classification of information catalogs the sensitivity of information assets

### Commercial

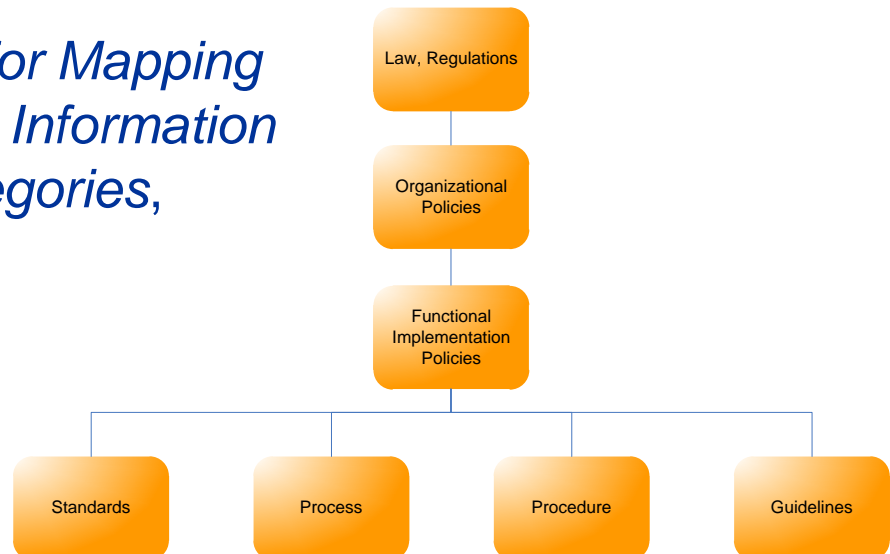
- Public
- Private / Sensitive
- Confidential / Proprietary

### Military and Civil Gov.

- Unclassified
- Controlled Unclassified Information (CUI)
- Confidential
- Secret
- Top Secret

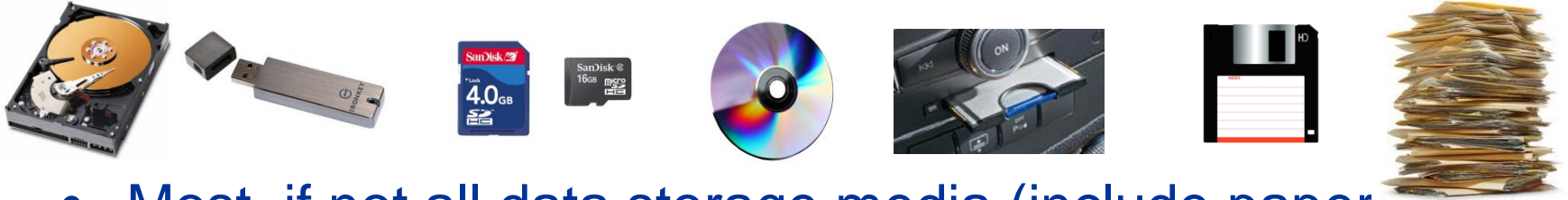
# Protection of Information ...<sup>(2/2)</sup>

- Operations must understand the relationships between policy, instruction, and guideline. Ex.:
  - E.O. 13526, E.O. 13556 (Whitehouse)
  - DoD 5200.01-M, *Information Security Program* (DoD Manual)
  - NIST SP 800-59, *Guideline for Identifying an Information System as a National Security System* (NIST guideline for civilian agencies)
  - NIST SP 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*, Vol. 1: Guide.



## Example: Protection of Media

---



- Most, if not all data storage media (include paper document) are “mobile”, except...
- Protection includes:
  - Marking & labeling of media
  - Handling of media
    - Transport
    - Access
    - Integrity of media



## Example: Protection of IT Assets

---




- Similar to data storage media, operations also deals with protection of IT assets (computing, network, and mobile platforms)
- Protection includes:
  - Asset inventory management (know what you have)
    - Hardware, software, and virtual machine configuration items (HWCIs, SWCIs, and VMCI)
  - Configuration management (know how they are configured)
    - 80-90% of known vulnerabilities can be attributed to misconfigurations and missing patches
  - Incident management



# Operations Security Domain

---

- Concept & Definition
- Identification of Resource Protection Needs
-  Threats to Information Operations
- Security Controls & Countermeasures

# Threat Agents ...(1/5)

- Threat sources varies, but “insider” and business partners are a great concern ...
  - In 2008, CSO Magazine reported:

Source of Incidents	2007	2008
Unknown	N/A	42%
<b>Employees</b>	48%	34%
Hackers	41%	28%
<b>Former employees</b>	21%	16%
Business partner	19%	15%
Customer	9%	8%
Other	20%	8%
Terrorist/ foreign government	6%	4%

- In 2009, Verizon Data Breach Investigation Report:

Source of Data Breach Incidents	2008	2009
External threat sources	73%	74%
<b>Insiders</b>	18%	20%
Business partner	39%	32%
Involved multiple parties	30%	39%

**Reference:**

- The Global State of Information Security 2008. *CSO Online*.
- *Verizon 2009 Data Breach Investigations Report*

## Threat Agents ...<sup>(2/5)</sup>

---

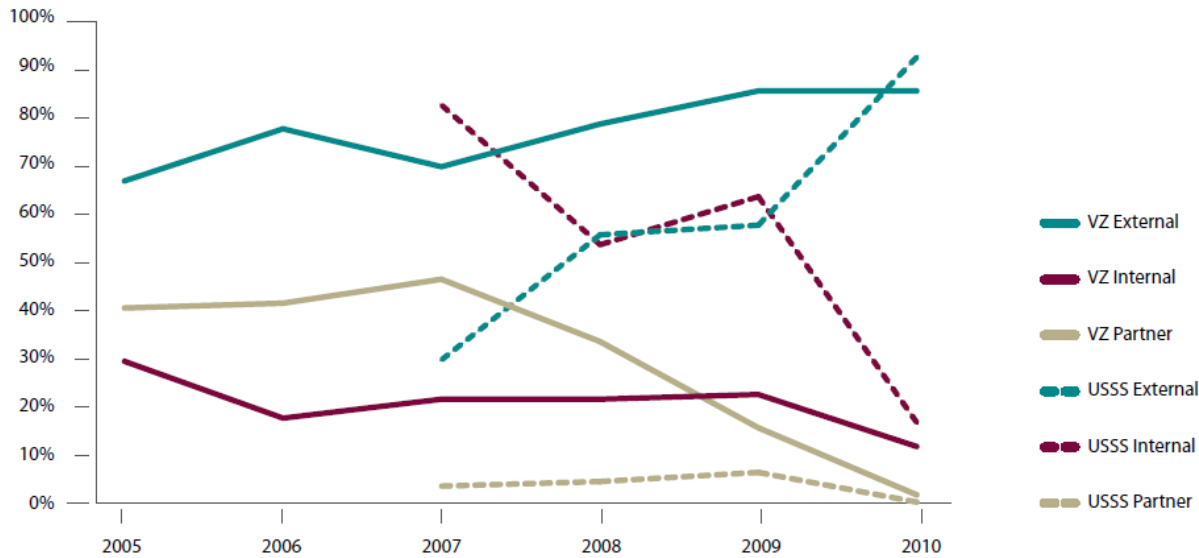
- In 2009, a CERT/SEI CyLab study found that:
  - 68% of the insider attack occurred at the workplace
  - 73% of crimes were committed during working hours
  - Over 3/4 of the insider had authorized access to information assets
  - None of the insider had privileged access
  - 20% involved in theft of physical properties (e.g., document, laptops, PCs, removable media, etc.)

**Reference:**

- *Insider Theft of Intellectual Property for Business Advantage: A Preliminary Model*. CERT Program, Software Engineering Institute and CyLab at Carnegie Mellon University, June 2009

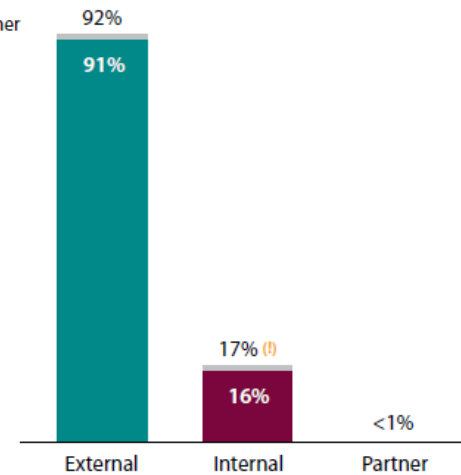
# Threat Agents ... (3/5)

- Operations are getting better at addressing insider threats



- VZ (Verizon)
- USSS (United States Secret Service)

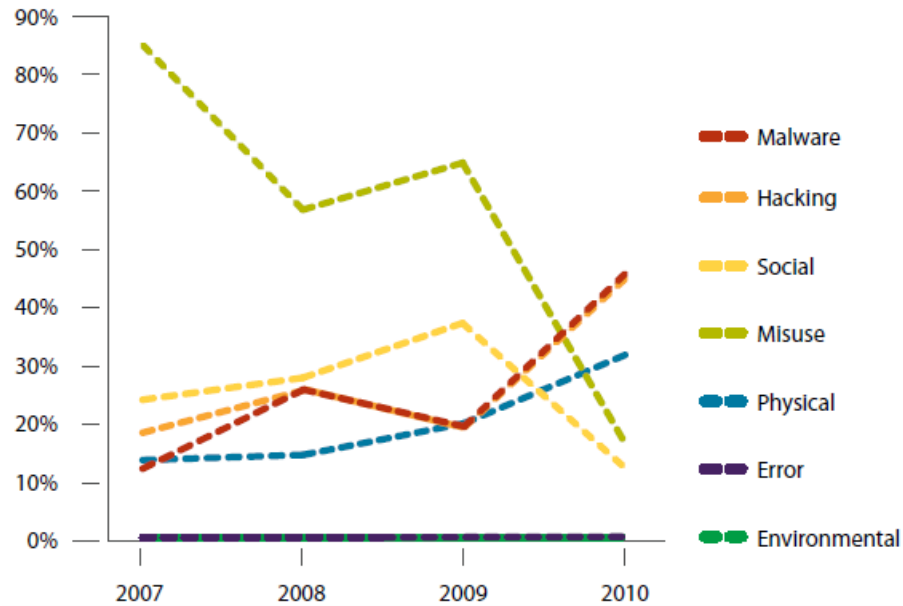
- Most of threats are from external threat agents



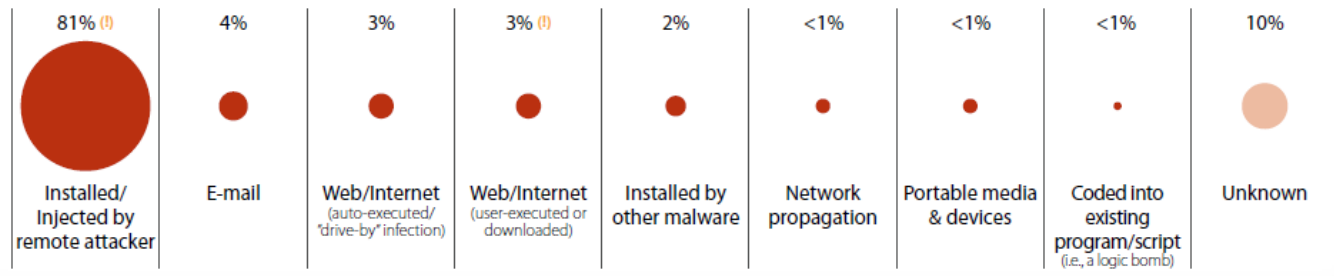
Reference: 2011 Data Breach Investigations Report, Verizon, January 2012  
([http://www.verizonbusiness.com/resources/reports/rp\\_data-breach-investigations-report-2011\\_en\\_xg.pdf](http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2011_en_xg.pdf))

# Threat Agents ... (4/5)

- Most of data breaches are from hacking and malware...



- Majority of malware are installed remotely...

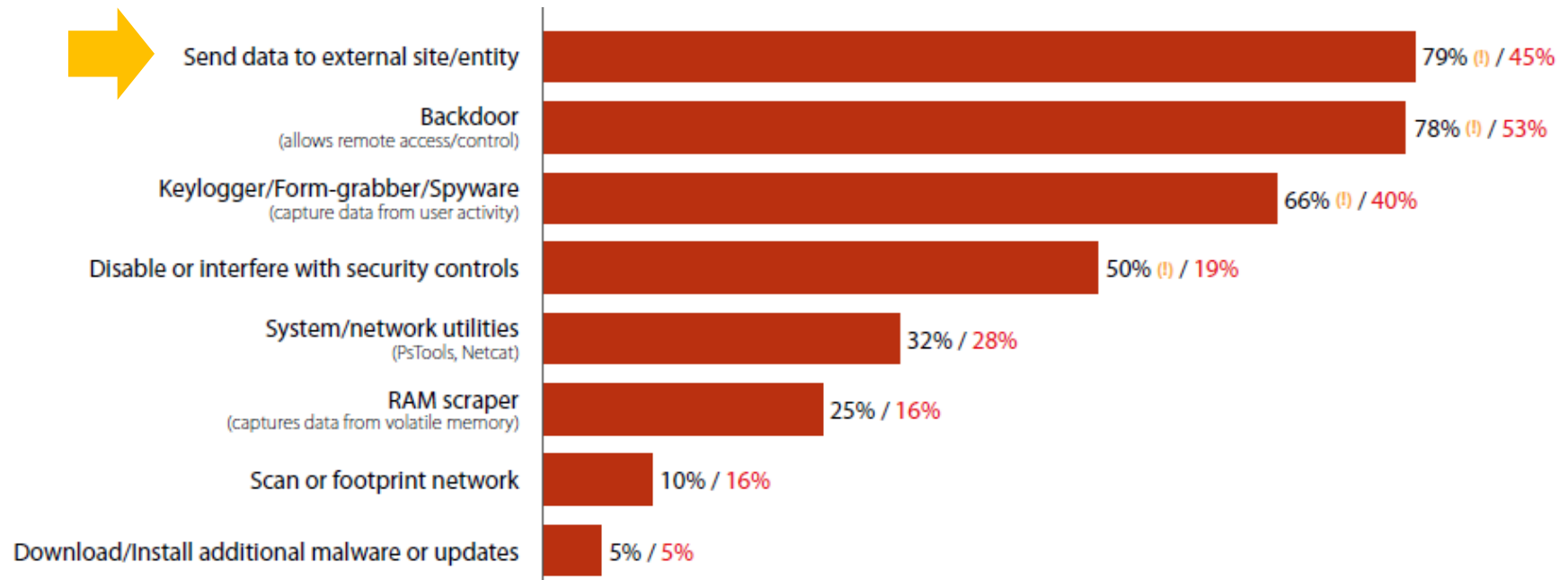


Reference: 2011 Data Breach Investigations Report, Verizon, January 2012

([http://www.verizonbusiness.com/resources/reports/rp\\_data-breach-investigations-report-2011\\_en\\_xg.pdf](http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2011_en_xg.pdf))

# Threat Agents ... (5/5)

- Advanced Persistent Threat (APT) is very real
  - Malware is now a tool for hackers
  - They are stealing data...



Reference: 2011 Data Breach Investigations Report, Verizon, January 2012

([http://www.verizonbusiness.com/resources/reports/rp\\_data-breach-investigations-report-2011\\_en\\_xg.pdf](http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2011_en_xg.pdf))

## Types of Threats ...(1/2)

---

- Theft / unauthorized configuration change
  - Lost of information assets or computing equipment
- Corruption / unauthorized modification
  - Unauthorized changes to file permissions, data, or system configuration (software, hardware or firmware).
- Unauthorized disclosure
  - Release of information to unauthorized subject(s).
  - Insider threats, where subjects with privileged access can compromise “need-to-know”.

## Types of Threats ... (2/2)

---

- Unauthorized destruction
  - Obliteration of information assets (e.g. deletion of data files, modification of log files) or destruction of computing equipment.
- Service interruption / denial-of-services
  - Personnel with privileged access may accidentally or intentionally disable or disconnect computing/networking equipment.



# Operations Security Domain

---

- Concept & Definition
- Identification of Resource Protection Needs
- Threats to Information Operations
- ➔ Security Controls & Countermeasures

# Security Controls – Federal Information Systems

CLASS	FAMILY	IDENTIFIER
Management	Risk Assessment	RA
	Planning	PL
	System and Services Acquisition	SA
	Certification, Accreditation, and Security Assessment	CA
	Program Management	PM
Operational	Personnel Security	PS
	Physical and Environmental Protection	PE
	Contingency Planning	CP
	Configuration Management	CM
	Maintenance	MA
	System and Information Integrity	SI
	Media Protection	MP
	Incident Response	IR
	Awareness and Training	AT
Technical	Identification and Authentication	IA
	Access Control	AC
	Audit and Accountability	AU
	System and Communications Protection	SC

Reference: NIST SP800-53, Rev.3, Recommended Security Controls for Federal Information Systems

# Security Controls – Commercial Information Systems

## ISO/IEC 27001:2005, *Information Technology – Security Techniques – Security Management System – Requirements*

CONTROL CATEGORIES	SUB-CATEGORY OF CONTROLS
Security Policy	Information security policy
Organization of Information Security	Internal organization; External parties
Asset Management	Responsibility for assets; Information classification
Human Resource Security	Prior to employment; During employment; Termination or change of employment
Physical and Environmental Security	Secure areas; Equipment security
Communications and Operations Management	Operational procedures and responsibilities; Third party service delivery management; System planning and acceptance; Protection against malicious and mobile code; Back-up; Network security management; Media handling; Exchange of information; Electronic commerce services; Monitoring
Access Control	Business requirement for access control; User access management; User responsibilities; Network access control; Operating system access control; Application and information access control; Mobile computing and teleworking
Information Systems Acquisition, Development, and Maintenance	Security requirements of information systems; Correct processing in applications; Cryptographic controls; Security of system files; Security in development and support processes; Technical vulnerability management
Information Security Incident Management	Reporting information security events and weaknesses; Management of information security incidents and improvements
Business Continuity Management	Information security aspects of business continuity management
Compliance	Compliance with legal requirements; Compliance with security policies and standards, and technical compliance; Information system audit considerations

## Example Directive Controls for Operations – DoD

---

- DoDD 5200.1, *DoD Information Security* defines the roles and responsibilities of operational organizations.
- DoD 5200.1-M, *Information Security Program* prescribes rules for implementation operations security within DoD.
- DoDD O-8530.1, *Computer Network Defense (CND)* defines the roles and responsibilities of DoD operational organizations for conducting CND.
- DoDI O-8530.2, *Support to Computer Network Defense (CND)* defines the operational process for conducting CND.
- DoDD 5200.2, *DoD Personnel Security* defines the personnel security program for DoD.

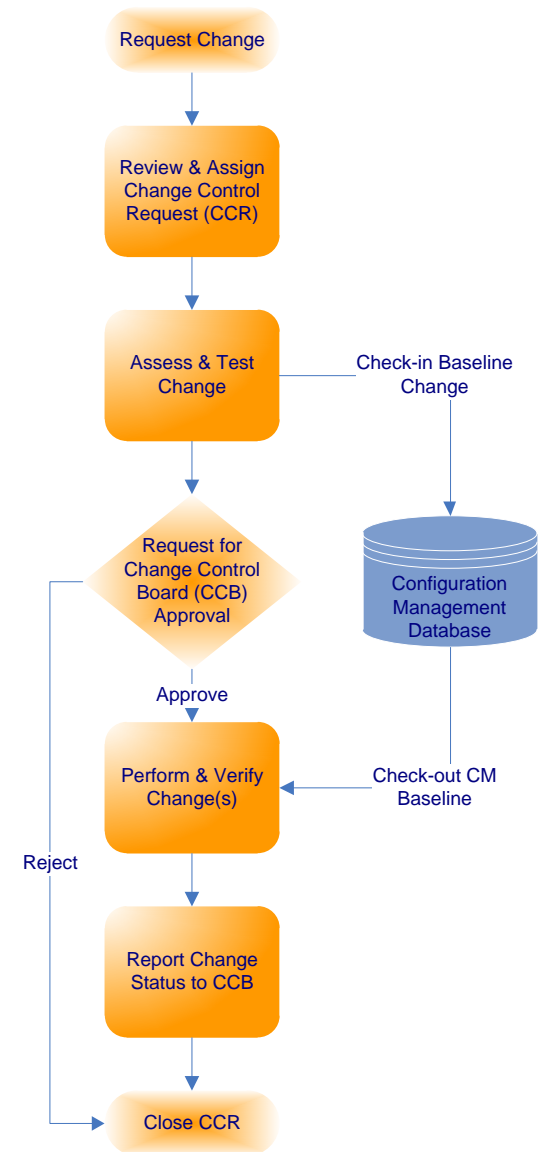
# Controls for Personnel Security

---

- Directive controls:
  - Define personnel security policy and procedures.
  - Define job functions (roles) and responsibilities (e.g. position categorization).
- Preventive controls:
  - Personnel screenings.
    - Background investigations, adjudications, and
    - User authorization and user agreements (e.g. NDA, Rules of Behavior).
  - Personnel transfer procedure to review roles & responsibilities.
  - Personnel termination procedure (e.g. Exit interview).
- Detective controls:
  - Periodic re-investigations.
- Corrective controls:
  - Personnel sanctions.

# Controls for Configuration Management

- Directive controls:
  - Configuration management policy and procedures,
  - Define configuration change control procedure.
- Preventive controls:
  - Baseline configuration (before change),
  - Test change (in test environment), and
  - Access restrictions for change (for trusted distribution).
- Detective controls:
  - Verify and validate change, and
  - Monitor configuration changes.
- Recovery controls:
  - Baseline configuration (after change), and
  - Trusted recovery.



# Contingency Planning ...(1/2)

---

- Directive controls:
  - Contingency planning policy and procedures.
- Preventive controls
  - Contingency planning
    - Address roles, responsibilities and define “chain-of-command”/reporting structure.
    - Align objectives with Business Continuity Planning (BCP), using Business Impact Assessment (BIA).
    - Coordinate planning with disaster recovery, COOP and incident response.
  - Contingency training
    - Cross-functional training on various roles. (Job rotation)
  - Perform information system backups (level 0: full, partial, and incremental).

# Contingency Planning ... (2/2)

---

- Detective controls
  - Contingency plan testing
    - Walkthroughs (tabletop exercise), checklist, simulation, or full interruption test.
- Corrective controls:
  - Perform contingency plan update to ensure alignment with business objectives and configuration change.
- Recovery controls:
  - Information system recovery and reconstruction.
    - Perform trusted recovery,
    - Retrieve backups from storage sites (primary, alternate),
    - Alternate processing sites, and
    - Restore or enable alternate telecommunication services.



## Contingency Planning – Categories of Recovery Actions

---

- Soft reboot (a.k.a. warm reboot). Restarting a system after shutting it down in a controlled manner.
- Random reboot (a.k.a. panic reboot, emergency system restart). Unintended reboot of a system after it fails in an uncontrolled manner in response to a security kernel or media failure.
- Hard reboot (a.k.a. cold start). When power to a computer is cycled. This is performed when unexpected security kernel or media failure occurs and the automated recovery procedures cannot bring the system back to a consistent state.

## Contingency Planning – Types of System Recovery

---

- Manual recovery allows an evaluated product to only provide mechanisms that involve human intervention to return to a secure state.
- Automated recovery provides for a least one type of service discontinuity recovery to a secure state without human intervention.
- Automated recovery without undue loss provides for automated recovery but strengthens the requirements by disallowing undue loss of protected objects.
- Function recovery provides for recovery at the level of particular security functions. It should ensure either successful completion of the security function or rollback to a secure state.

## Contingency Planning – Data Backups ... (1/4)

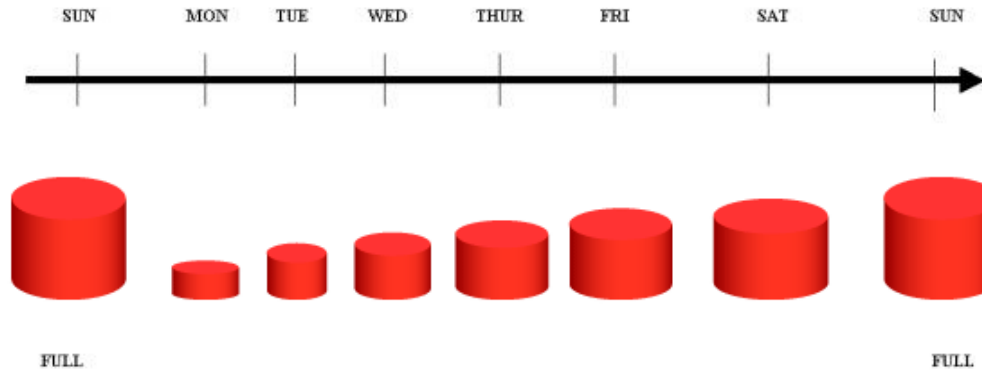
---

Three types of data backups:

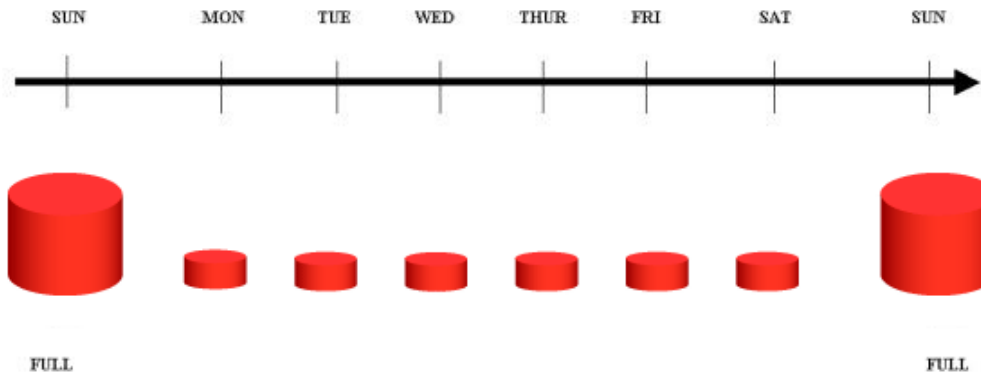
- Full volume backup is backup performed on an entire disk volumes of a system(s).
- Differential backup is a backup of changes since last full backup, but does not change the archive bit value.
- Incremental backup is a backup of changes since last full or incremental backup and sets the archive bit to 0.

# Contingency Planning – Data Backups ... (2/4)

- Recovery steps: Full + differential backup.

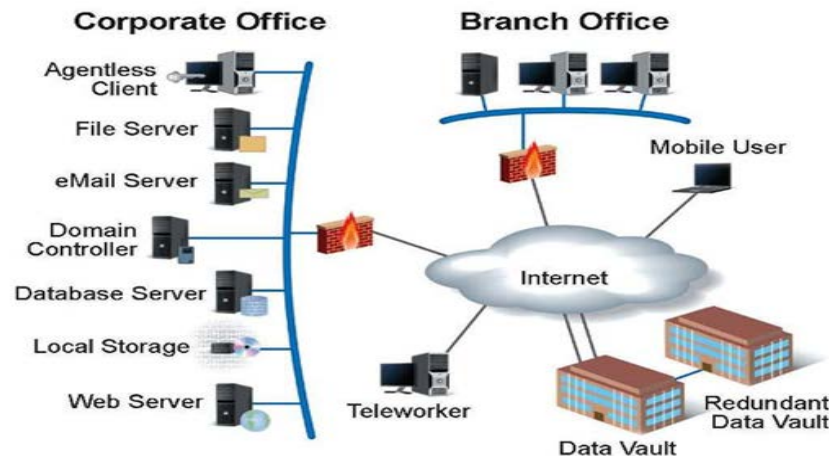


- Recovery steps: Full + sequence incremental backups

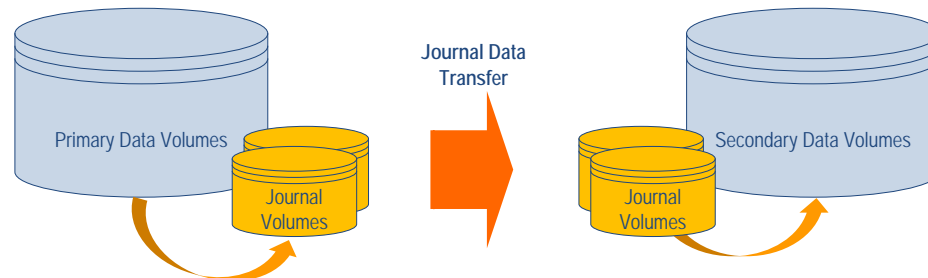


# Contingency Planning – Data Backups ... (3/4)

- Three types of electronic vaulting:
  - Online tape vaulting: Data is transported through a trusted communications channel to a tape backup service.

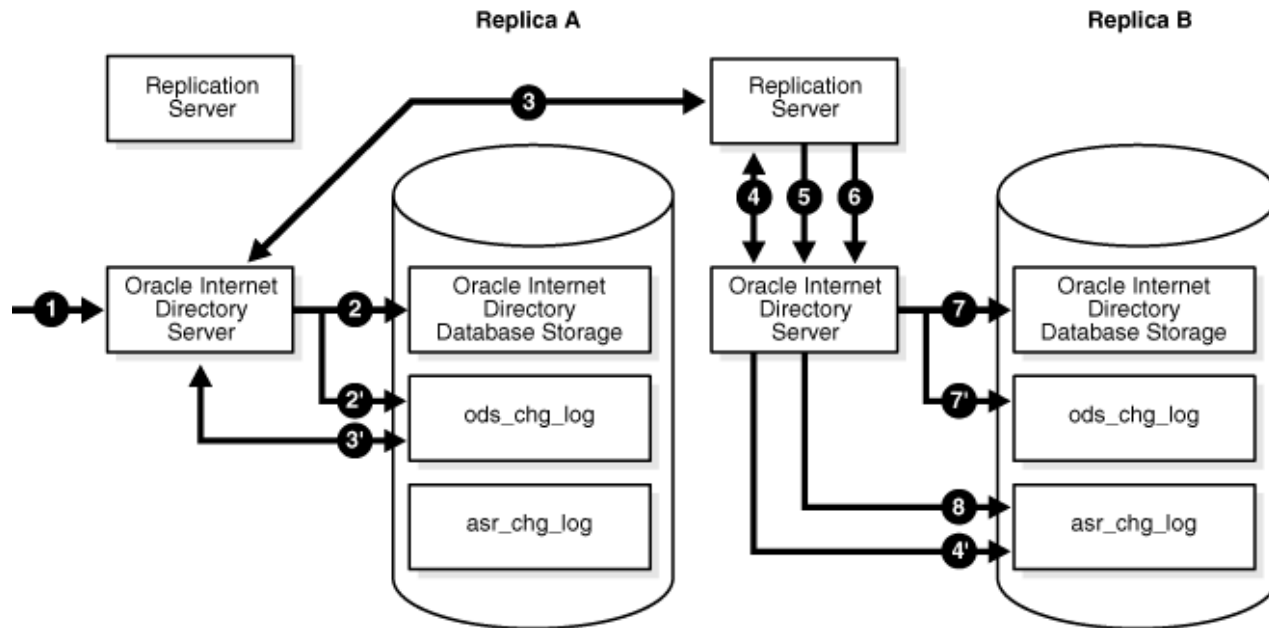


- Remote transaction journaling: Journal of transactions are created in the primary system and sent to the secondary system.



# Contingency Planning – Data Backups ... (4/4)

- Three types of electronic vaulting:
  - Database shadowing (a.k.a. database replication): System updates the primary data volume, journals them, then send them to the secondary system.



## Controls for Maintenance ... (1/2)

---

- Directive controls:
  - System maintenance policy and procedures.
- Preventive controls:
  - Periodic maintenance
    - Keep inventory records for baseline configuration so organization may schedule and perform preventive or regular maintenance.
    - Keep maintenance records of each system component.
  - Utilize maintenance tools to:
    - Monitor & track inventory & maintenance records
    - Monitor & track service level and mean time between failure (MTBF) of system or components.
    - Use workflow tools to facilitate change control and CM tools to track baseline.

## Controls for Maintenance ...(2/2)

---

- Preventive controls:
  - Remote maintenance
    - Ensure remote maintenance is performed under monitor & control, and it is executed in accordance to change control process.
  - Maintenance personnel
    - Ensure only authorized personnel can access systems
    - Use “least privilege” principle when assign access levels to a specific role.
    - Keep track of authorized 3<sup>rd</sup> party maintenance personnel and document actions performed.
  - Ensure timely maintenance
    - Define & monitor service level agreements (SLAs)
    - Keep or arrange supply chain of spare parts for mission critical components.



## Questions:

---

- What is the difference between due care and due diligence?
  - 
  -
- Estimate for the lifespan of a computing equipment is?
  -
- Estimate for the amount of time to repair a computing equipment is?
  -

## Answers:

---

- What is the difference between due care and due diligence?
  - Due care is actions taken
  - Due diligence is continual actions
- Estimate for the lifespan of a computing equipment is?
  - Mean Time Between failures (MTBF)
- Estimate for the amount of time to repair a computing equipment is?
  - Mean Time To Repair (MTTR)

## Questions:

---

- Recovery that involves human intervention to return a system back to a secure state is called?
  -
- Automated system recovery without undue loss is called?
  -
- What are the three types of data backup?
  - 
  - 
  -

## Answers:

---

- Recovery that involves human intervention to return a system back to a secure state is called?
  - Manual recovery
- Automated system recovery without undue loss is called?
  - Automated recovery without undue loss
- What are the three types of data backup?
  - Full volume backup
  - Differential backup
  - Incremental backup

## Controls for System and Information Integrity...(1/2)

---

- Directive controls:
  - System and information integrity policy and procedures.
    - Define users (non-privilege & privilege) rules of behavior
    - Define systems rules of behavior
- Preventive controls:
  - “Harden” systems
  - Malicious code protection: periodic update of anti-virus signatures
  - Intrusion prevention tools & techniques (IPS, file integrity tools)
  - Issuance of security alerts and advisories (situation awareness)
  - Information records handling and retention
    - CM system baseline (i.e. hardware configuration items (CI's) & software CIs)
    - System log retention

## Controls for System and Information Integrity...(2/2)

---

- Detective controls:
  - Intrusion detection tools & techniques.
  - Monitor system changes.
  - Monitor user access (non-privilege & privilege).
  - Security functionality verification
    - Security audits for compliance.
    - Periodic security assessments (to identify potential vulnerabilities & mitigate potential exposure).
- Corrective controls:
  - Practice change control for change management.
  - Limit access to CM library of baseline configuration.
- Recovery controls:
  - Perform trusted recovery.
  - Obtain baseline from CM.

# Controls for System and Information Integrity – Redundant Array of Inexpensive Disks (RAID)

- RAID Level Descriptions

RAID Level	Description
0	<u>Striping</u> . Stripes data across all disks.
1	<u>Mirroring</u> . Mirroring data from one disk to another (i.e. hot spare).
2	<u>Hamming code parity</u> . Bit-interleaves data across multiple disks with error correcting code (ECC) created using a Hamming code.
3	<u>Byte level parity</u> . Stripes data across multiple drives & write parity to a dedicated drive.
4	<u>Block level parity</u> . Stripes data across multiple drives & write parity to a dedicated drive.
5	<u>Interleaved parity</u> . Stripes data & parity information at block level.
6	<u>Second parity data (or double parity)</u> . A second set of parity data written on all drives
10	<u>Striping and mirroring</u> . Data are simultaneously mirrored and striped (RAID 0+1) across several drives and can support multiple drive failures

# Media Protection

---

- Directive controls:
  - Media protection policy and procedures.
  - Define information classifications (i.e. unclassified, confidential, secret, top secret, or SCI).
- Preventive controls:
  - Media labeling.
  - Limit media access in accordance to “need-to-know”, and “least privilege” principles.
  - Define media storage: encryption, location, environment (on-site, off-site), storage period.
  - Define media transport procedure (i.e. handling of FOUO, Classified information: SCI, NOFORN).
  - Media sanitization (Not delete, but overwrite or degauss).
  - Media destruction and disposal.



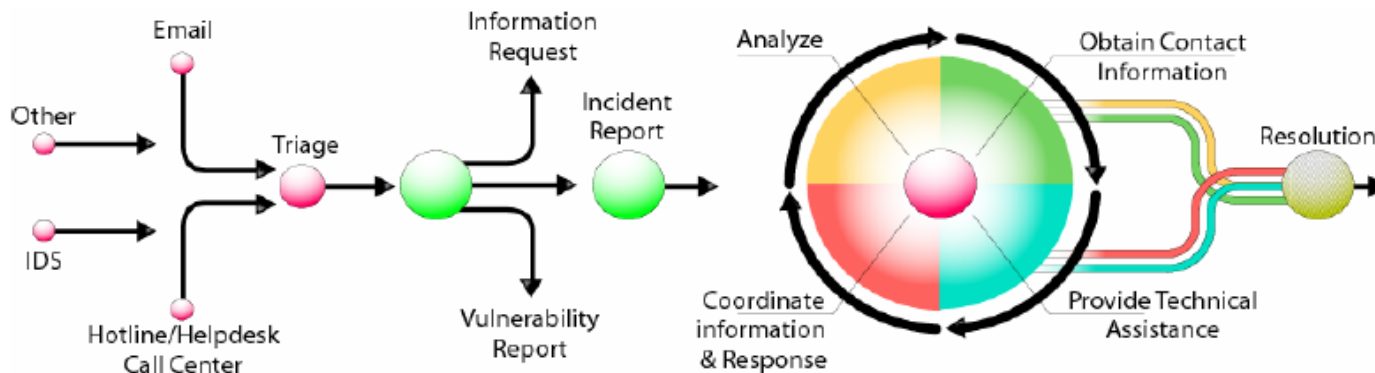
# Incident Response ... (1/2)

---

- Directive controls:
  - Incident response policy and procedures.
  - Create a Computer Security Incident Response Team (CSIRT/CIRT/CERT).
  - Define levels of security response measures to maintain security posture. (e.g. INFOCON).
- Preventive controls:
  - Incident response training
    - Know the incident response process, procedure, and standard response measures (Tier 1: Operator, call center; Tier 2: Helpdesk, NOC, SOC; Tier 3: CSIRT, system engineers).
    - Professional training & education: technical, interpersonal, and managerial skills.
  - Incident response testing
    - Practice change control process, follow CM policy.

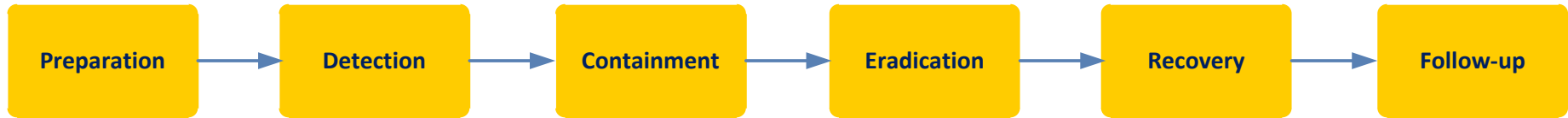
# Incident Response ... (2/2)

- Detective controls:
  - Incident monitoring
    - Define event severity, associate & correlate syslogs, event logs, access logs, firewall, IDS, anti-virus system logs.
    - Document events and security incidents. Preserve evidence.
- Corrective controls:
  - Incident handling.
  - Incident reporting.
  - Incident response assistance.



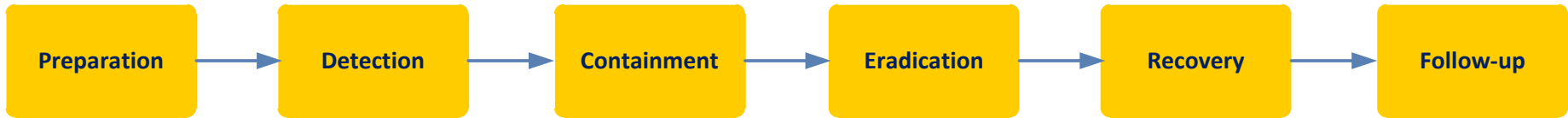
# Incident Response – Life Cycle ... (1/3)

---



- Preparation
  - Concept of operations
  - Service functions and definitions
  - Processes and procedures
  - Organizations & personnel
  - Technology and communications Infrastructure
- Detection
  - Detection systems (detection of security events)
  - Monitoring systems (monitoring of security controls)
  - Reporting systems (incidents)

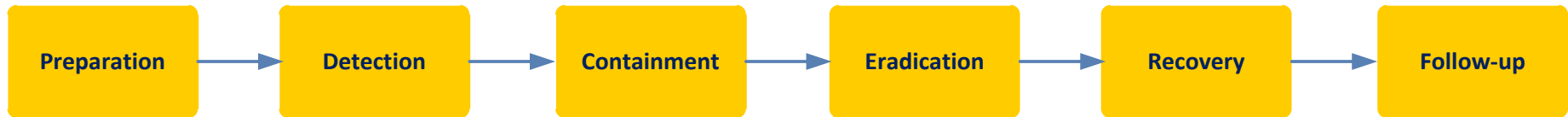
# Incident Response – Life Cycle ... (2/3)



- Containment
  - Containment strategy
  - Logics in containment (condition-based response level, ex. INFOCON)
  - Processes & procedures (coordinated response)
- Eradication
  - Analyze the problem (investigation, assess impact & severity)
  - Mitigate the problem (remediate, test, and document procedure)
  - Communicate “change” and “clean-up”

## Incident Response – Life Cycle ...<sup>(3/3)</sup>

---



- Recovery (SOC is not a bunch of “cyber janitors”)
  - Coordinate & perform recovery processes (technology, data, and business) (See BCP/DRP domain)
  - Conduct audits and security tests
  - Return to normal operations
- Follow-up
  - Conduct analysis to prevent repeat incident (i.e., lessons-learned)
  - Propose countermeasures and preventive measures
  - Plan and implement countermeasures

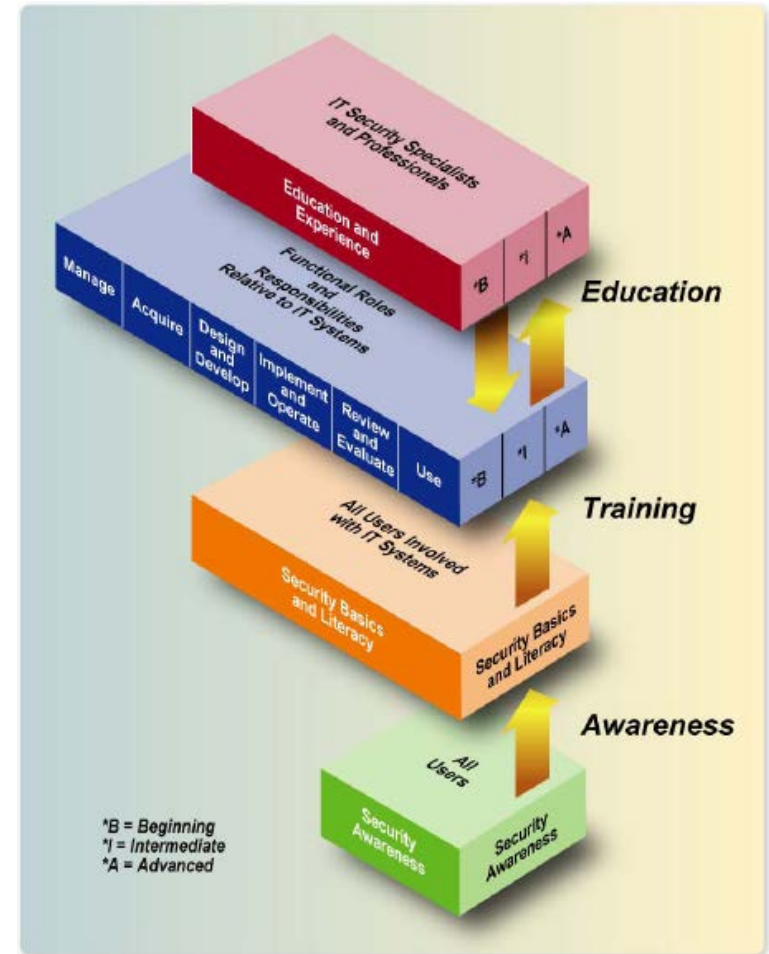
# Incident Response – Organizational Structure

---

- “Form follows function”
  - Organizational structure of an effective computer (/cyber) security incident response team (CSIRT) should always follow mission needs
  - Examples CSIRT organizational model:
    - Central (for highly integrated organization)
    - Distributed (for hierarchical, large enterprise), or
    - Coordinated (for multiple, federated, autonomous enterprises)
- Functions, activities, and tasks
  - Function is organized based on activities and tasks:
    - Triage (helpdesk, call centers) (Tier 1)
    - Investigation and containment (Tier 2)
    - Analysis and eradication (Tier 3)
    - Recovery, engineering of countermeasures, testing
    - Follow-up, planning, and prevention

## Awareness and Training... (1/2)

- Directive controls:
  - Security awareness and training policy and procedures.
  - Define training needs in accordance with roles & responsibilities.
  - Professionalize discipline by certification.
- Preventive controls:
  - Security awareness (All users).
  - Security training (based on roles & responsibilities).
- Corrective controls:
  - Keep track of security training records to ensure quality of workforce.



## Awareness and Training... (2/2)

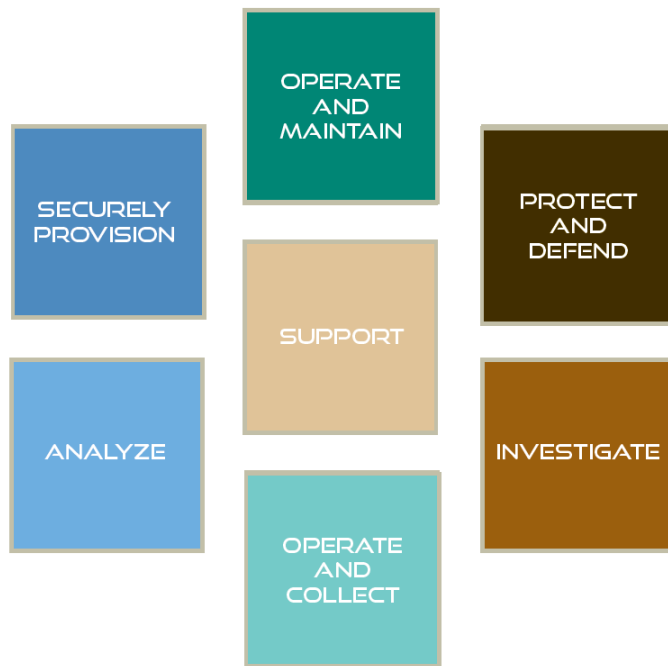
---

- NIST SP 800-50 defined three components to an IT information security training program:
  - Security awareness trainings are designed to:
    - Communicate management's goals and expectation for the protection of organization's information assets.
    - Review the rule of behavior for securing information assets.
  - Role-based security trainings are designed to:
    - Provide specific job skills for a specific job function.
  - Security education is to:
    - provide personnel with knowledge specialize in information security.



# Security Training and Education – the National Initiative for Cybersecurity Education (NICE) ... (1/2)

- NICE is a part of Comprehensive National Cybersecurity Initiative (CNCI) where government and industry collaborated to create a training & educational framework for cybersecurity workforce.



CYBERSECURITY  
**WORKFORCE**  
FRAMEWORK

# Security Training and Education – the National Initiative for Cybersecurity Education (NICE) ...<sup>(2/2)</sup>

<b>Securely Provision</b>	Specialty areas concerned with conceptualizing, designing, and building secure IT systems.
<b>Operate and Maintain</b>	Specialty areas responsible for providing the support, administration, and maintenance necessary to ensure effective and efficient IT system performance and security.
<b>Protect and Defend</b>	Specialty area responsible for the identification, analysis and mitigation of threats to IT systems and networks.
<b>Investigate</b>	Specialty areas responsible for the investigation of cyber events or crimes which occur within IT Systems and networks.
<b>Operate and Collect</b>	Specialty areas responsible for the highly specialized and largely classified collection of cybersecurity information that may be used to develop intelligence.
<b>Analyze</b>	Specialty area responsible for highly specialized and largely classified review and evaluation of incoming cybersecurity information.
<b>Support</b>	Specialty areas that provide critical support so that others may effectively conduct their cybersecurity work.

## Questions:

---

- What type of security control is intrusion detection?
  -
- Trainings that communicate management goals and expectations for protection of information assets are?
  -
- Trainings that enables an employee to perform his/her assigned security responsibilities are?
  -

## Answers:

---

- What type of security control is intrusion detection?
  - Detection control
- Trainings that communicate management goals and expectations for protection of information assets are?
  - Security awareness trainings
- Trainings that enables an employee to perform his/her assigned security responsibilities are?
  - Role-based security trainings

---

# BACKGROUND STUDY

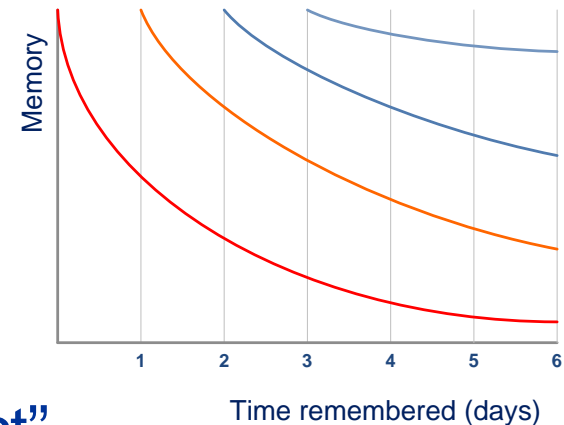
# Case Study 1: Effectiveness of Annual Security Awareness Training

---

- In 2007, TIGTA conducted an audit on the effectiveness of IRS Annual Security Awareness Training – UNAX...
- Attack Method: Social Engineer
  - Auditor posed as IT helpdesk personnel seeking assistance to correct a network problem.
  - Users were requested to change their passwords to the ones TIGTA auditor had suggested.
- Result:
  - 60% IRS employees had bought-in on the social engineering attack and changed their passwords
  - 20% IRS employees cited awareness training as the primary reason for not buy-in on the social engineering attack
  - In 2001, 70% IRS employees had bought-in on the same social engineering attack.

# Case Study 1: People forget what they've learned

- In 1870, Hermann Ebbinghaus pioneered an experimental study – “Forgetting Curve”
  - 2/3 of student retained the learned knowledge after an hour
  - 28% remember the specifics in 2 days
- However, if the learned knowledge is re-enforced in the following day, more students were able to remember what they've learned. – “Spacing Effect”



## Case Study 2: Effectiveness of security awareness training re-enforced with “hands-on” exercises

---

- In 2005, United States Military Academy (USMA) at West Point conducted a proof-of-concept on the effectiveness of their security awareness training...
  - Per semester, all cadets receive security awareness training
  - Every freshman were subjected to a 4-hr. security awareness course
- Attack Method: Social Engineering
  - A “phishing” e-mail message from a fictitious US Army colonel
  - E-mails informed cadets of a problem with their current grade report and instructed them to click on the embedded hyperlink
- Results:
  - 80% (over 400) cadets clicked on the embedded hyperlink
  - 90% of freshmen –with 4 hrs training- clicked on the link



## Case Study 2: How people learn

---

- In 1918, Edward Thronthike defined a set of “Learning Principles”
  - The most basic form of learning is trial and error learning
  - Law of exercise: We learn by doing, we forget by not doing
    - Law of use: Connection between a stimulus and a response are strengthened as they are used
    - Law of disuse: Connection between a stimulus and a response are weakened as they are not used
  - Law of effect: If the response in a connection is followed by a satisfying state of affairs, then the strength of connection is considerably increased. (Positive reinforcement)
- West Point considered the study a success...
  - Approved for USMA-wide deployment (4,400 Corps of Cadets)
  - Added 3 additional variants

## Case Study 3: A comparative study between game- and video-based security awareness training

---

- In 2009, Jonathan Jones, et. al. conducted a pilot study comparing the educational effectiveness of:
  - Game-based security awareness training – CyberCIEGE
  - Video-based DoD IASE Information Assurance Awareness (DoD IAA) Training Course
- Study:
  - Pre-tests conducted to establish the baseline
  - Post-tests conducted 2 weeks after to measure effectiveness of student's learning
- Result:
  - The average improvement of “game group” (40%) is higher than the “video group” (33%)
  - On average, “game group” had spent much more time (6.15 hr.) than the “video group” (1.75 hr.)

## Case Study 3: Repeated learning with positive reinforcement

---

- In 1965, Jean Piaget formalized the learning theory of “Constructivism”
  1. People learn to learn as they learn: learning consists both of constructing meaning and constructing systems of meaning.
  2. The crucial action of constructing meaning is mental: it happens in the mind. Physical actions, hands-on experience may be necessary for learning
- Learning Principles: Laws of effect.
  - Positive feedback is rewarding

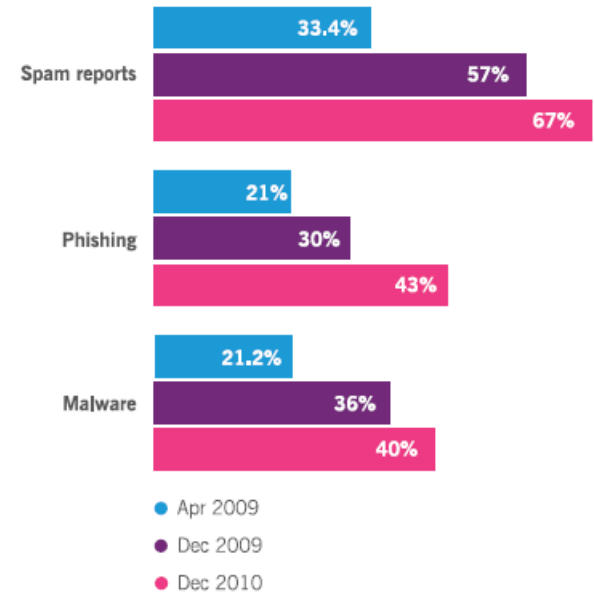
## Case Study 4: New technology but same operational issues

- In early 2010, Cisco Systems published a study on top security issues in 2009.
- Top security issue:
  - Social networking media that uses Web 2.0 technologies became the new attack vector.
- Method: Social Engineering
  - Relying on social networkers' willingness to respond to phishing messages originate from people they know and trust
  - Threat vector:
    - Twitter message with embedded hyperlink from TinyURL.com (URL redirection service) that leads to malicious websites
    - Facebook e-mail messages from a friend with embedded link that leads to malicious websites requests to download malware
    - Password reuse between Gmail, Yahoo, Facebook, Twitter, etc.

# Social Engineering Simply Works ...

- Social engineering techniques now works even better through social networking services
  - Facebook
  - Twitter
  - LinkedIn

Social networks Spam, Phishing and Malware reports up



Source: Sophos Survey December 2010

Do you think your employee's behavior on social networking sites could endanger security at your company?



• No 41%  
• Yes 59%

Source: Sophos Survey December 2010

Reference: Sophos Security Threat Report 2011, January 2011