



# Operations and Incident Response

Domain 4 – 16%




1

1

## SECURITY GOVERNANCE

Align security function to:

- Strategy - well defined steps for mission
- Goals - intermediate term
- Mission - long term
- Objectives - milestone short term



Consider:  
Business case  
Budget  
Resources

2

2

# Security Management

- Policies
- Standards
- Baselines
- Guidelines
- Procedures



Apply security governance principles through Organization Processes

- Acquisitions
- Divestitures
- Governance committees



3

## Security Management Examples

- IS Security Steering Committee
- The Audit Committee
- Security-Awareness Training
- Software Piracy (EULA)
- Acceptable Use Policies (AUP)



4

4

# Know Who You're Dealing With

Background Checks

Military Security  
Clearance

Hiring and Termination

Employment Agreement



5

5

## Background Checks

- It is important to properly screen individuals before hiring them into a corporation.
- These steps are necessary to help the company protect itself and to ensure it is getting the type of employee required for the job.
- Limitations exist regarding the type and amount of information that an organization can obtain on a potential employee.



Illustration by Chris Gash



6

6

## Employees

- Agreements and Policies



- Monitoring Employees

- ✓ Emails
- ✓ Web Browsing
- ✓ Door Badge Access

## Ethics

- Act honorably, honestly, justly, responsibly, and legally, and protect society.
- Work diligently, provide competent services, and advance the security profession.
- Encourage the growth of research—teach, mentor, and value the certification.
- Discourage unnecessary fear or doubt, and do not consent to bad practices.
- Discourage unsafe practices, and preserve and strengthen the integrity of public infrastructures.
- Observe and abide by all contracts, expressed or implied, and give prudent advice.
- Avoid any conflict of interest, respect the trust that others put in you, and take on only those jobs you are fully qualified to perform.
- Stay current on skills, and do not become involved with activities that could injure the reputation of other security professionals.

IN YOUR COMMUNITY: JOBS • AUTOS • REAL ESTATE • RENTALS • CLASSIFIEDS • OBITUARIES • FIND&SAVE • LOCAL BUSINESSES • PLACE AN AD

**AL** All Alabama


Set Weather Search Sign in | Join

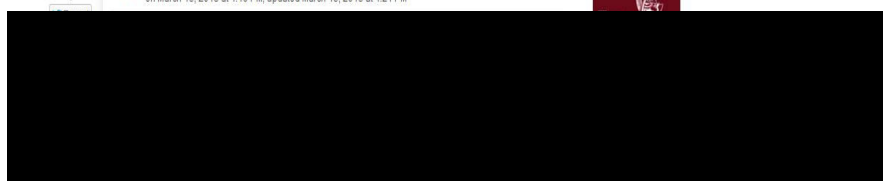
NEWS BUSINESS SPORTS H.S. SPORTS ENTERTAINMENT LIVING brought to you by: *gulf shores orange beach*


## 4 Spies in Huntsville? Believe it. FBI calls the city a 'major target' for espionage

By Lee Roop | lroop@al.com  
 Email the author | Follow on Twitter  
 on March 15, 2013 at 4:19 PM, updated March 15, 2013 at 4:21 PM

33

Print Sponsored By: 




 CyberProtex


9

9

# Computer Crimes



- Types
  - Computers as Target
  - Computers as Incidental to Crime
  - Computers as Instrument of a Crime
  - Crimes associated with Prevalence of Computers

 CyberProtex

10

10

## DEAR OL' MOM



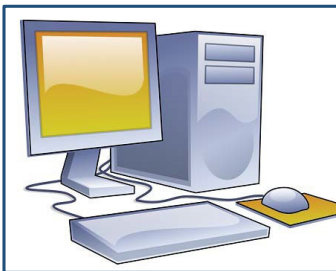
- **Motive**
- **Opportunity**
- **Means**



11

11

## Operation Strategy and Practice



Consider Security risk in all areas and generate countermeasures:

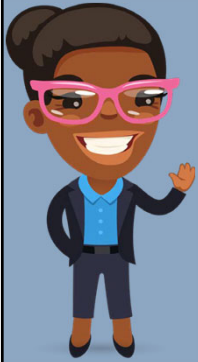
- Stand Operating Procedures (SOP) – day to day processes including hardware, software and services
- Third-party and outsourced services – legal department
  - ✓ On-site assessment
  - ✓ Document exchange and review
  - ✓ Process/policy review
- Service Level Agreements (SLA)
- Business Partners Agreement (BPA)
- Interconnection Security Agreement (ISA)
- Memorandum of Understanding (MOU)
- Memorandum of Agreement (MOA)



12

12

## Security Roles and Responsibilities



Role	Responsibilities/Duties
<b>Data Owner</b>	responsible for data security and sets relevant policies - business function
<b>Steward/Custodian</b>	responsible for day to day data interactions with the data and ensures policies set by the data owner are followed
<b>Privacy Officer</b>	responsible for establishing and enforcing data privacy policy
<b>System Administrator</b>	maintain the hosts within set requirements
<b>System Owner</b>	responsible for the overall operation of the data and application including security, privacy, and retention - business function
<b>User</b>	least amount of privileged access and restricted to mission
<b>Privileged User</b>	additional privileges for application and data access
<b>Executive User</b>	responsible for the overall operations



13

13

## Information security education, training, and awareness

- Establish appropriate levels of awareness, training, and education required for individual organization



- Review periodically for content relevancy and update as needed



14

14

## Ranking of Personnel Management

Access Control	Description	Rank	Justification
Least Privilege	Protects its most sensitive resources by ensuring that the individual should have only the necessary rights and privileges to perform her/his task	1	Easiest to implement and operating systems support available
Implicit Deny	If a situation is not covered by any of the rules, then access cannot be granted. An essential default setting for any security system. Any individual without proper authorization cannot be granted access. The alternative to implicit deny is to allow access unless a specific rule forbids it.	2	Third party software available to support, but requires forethought and is not the default setting
Separation of Duties	Term is applicable to physical environments as well as network and host security. For any given task, more than one individual is affected. A task is broken into different duties, each of which is accomplished by a separate individual.	3	Requires clean division duties and tasking not always found in small companies



15

15

## Ranking of Personnel Management

Access Control	Description	Rank	Justification
Job Rotation	Term defines the rotation of individuals through different tasks and duties. The rotation could occur at predetermined time intervals and prevent single point of failure	4	Requires multiple people with spin up time for training with every rotation
Mandatory Vacation	A mandatory vacation policy requires all users to take time away from work to refresh. Mandatory vacation give the employee a chance to refresh, but it also gives the company a chance to make sure that others can fill in any gaps in skills and satisfies the need to have replication or duplication at all levels. Mandatory vacations also provide an opportunity to discover fraud.	5	Requires adequate Personal Time Off (PTO) and two to three deep work force



16

16



## Example of Personnel Management

Access Control	Breach
Separation of Duties	In 2008, a breach at the Societe Generale ended costing the second largest bank in France \$7 billion. The fraudulent trading continued for over a year as Jerome Kerviel used insider knowledge to manipulate five levels of controls. Although separation of duties was in place, Kerviel had worked in middle management and was able to override the various controls not under his immediate jurisdiction. In addition, many in the oversight role did not know what controls were in place nor how these controls were to be implemented. In fact, several bank audits had failed to recognize the fraudulent activity.
Job Rotation	Disgruntled IT employee Terry Childs, blocked access to part of the city of San Francisco's network. Childs was a single point of failure as no one else had the passwords. The incident cost the city \$1.5 million dollars was paid as retribution by Childs. Childs also received a four-year prison sentence.



17

17

## Example of Personnel Management

Access Control	Breach
Least Privilege	In his role of technology analyst for the NSA, Edward Snowden accessed and copied an estimated 1.7 million NSA files while working in Hawaii as a contractor. In this case, least privilege access control was not implemented. In fact, in a recent survey, only 27% respondents blocked privileged user access to sensitive data.
Implicit Deny	J.P. Morgan's breach traced to a malware infection on one of their employee's computer. Application whitelisting would deny the malware from installing itself and prevented one of the largest breaches on an American bank to date.
Mandatory Vacation	Jerome Kerviel admitted he hadn't take one single day of vacation that year because he did not want anyone else to look at his books



18

18

# Risk Management And Assessment

- **Risk assessment**
  - ✓ Identify assets
  - ✓ Identify threats
  - ✓ Calculating risks
  
- **Qualitative and Quantitative Risk Analysis**
  
- **Delphi Technique**



19

19

# Business Impact Analysis (BIA)



- Evaluates the critical systems and functions for risks and losses (mission essential)
- Tangible and intangibles
- Calculates times you can do without
  - ✓ Maximum tolerable downtime (MTD)
    - Mean Time Between Failure (MTBF)
    - Mean Time To Failure (MTTF)
    - Mean Time To Restore (MTTR)
  - ✓ Recovery Time Objectives (RTO)
  - ✓ Recovery Point Objective (RPO)



20

20

# Risk Analysis

- Annualized loss expectancy (ALE)
- Annualized rate of occurrence (ARO)
- Exposure factor
- Probability
- Threat
- Safeguard
- Vulnerability

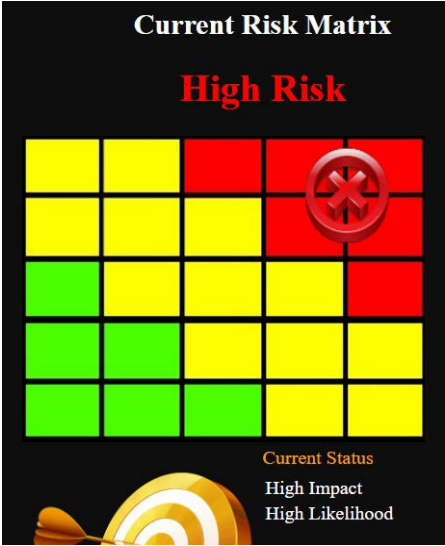


## Quantitative vs Qualitative Characteristics

Attribute	Quantitative	Qualitative
Requires no calculations		X
Requires more complex calculations	X	
Involves high degree of guesswork		X
Provides general areas and indications of risk		X
Is easier to automate and evaluate	X	
Used in risk management performance tracking	X	
Provides credible cost/benefit analysis	X	
Uses independently verifiable and objective metrics	X	
Provides the opinions of the individuals who know the processes best		X
Shows clear-cut losses that can be accrued within one year's time	X	

# Qualitative

Perform  
reduction  
analysis  
  
HEAT MAP



# Risk Assessments

- $SLE \times ARO = ALE$
- Prioritize threats, vulnerabilities, and impact of losses
- Enumerate through each risk
- Exposure of Company
- Reality Check
  - ✓ Risk assignment/acceptance



## Breaking Down How SLE and ALE Values Are Used

<b>Asset</b>	<b>Threat</b>	<b>Single Loss Expectancy (SLE)</b>	<b>Annualized Rate of Occurrence (ARO)</b>	<b>Annual Loss Expectancy (ALE)</b>
Facility	Fire	\$230,000	0.1	\$23,000
Trade secret	Stolen	\$40,000	0.01	\$400
File server	Failed	\$11,500	0.1	\$1,150
Data	Virus	\$6,500	1	\$6,500
Customer credit card info	Stolen	\$300,000	3	\$900,000

## Security Management

- Information security policies
- Assets
- Risks
- Threats
- Cost/benefit analysis
- Security awareness

## Apply risk management concepts



- Countermeasure selection
- Implementation
- Types of controls
  - ✓ Technical
  - ✓ Administrative
  - ✓ Physical
  - ✓ Deterrent
  - ✓ Preventive
  - ✓ Detective
  - ✓ Corrective
  - ✓ Compensating

## Security Controls

Control	Description
Technical	Using technology to address a physical security issue
Administrative	Policy or procedure to limit a security risk
Physical	Prevents physical action
Deterrent	Discourages an attacker by reduces the likelihood of success
Preventive	Prevents a malicious action from occurring by blocking or stopping
Detective	Helps to detect any malicious activities
Corrective	Attempts to get the system back to normal and reduce damage
Compensating	Restores but does not prevent an attack

## Data Sensitivity

Sensitivity Level	Description
Public	No restrictions
Private	Disclosure would cause harm or disruption to the organization
Confidential	Disclosure would cause serious harm to the organization
Proprietary	Property of the organization - trade secrets
Personally Identifiable Information (PII)	Data that can be used to identify an individual
Protected Health Information (PHI)	Health information of an individual

## Detecting Risks

### Internal Monitoring

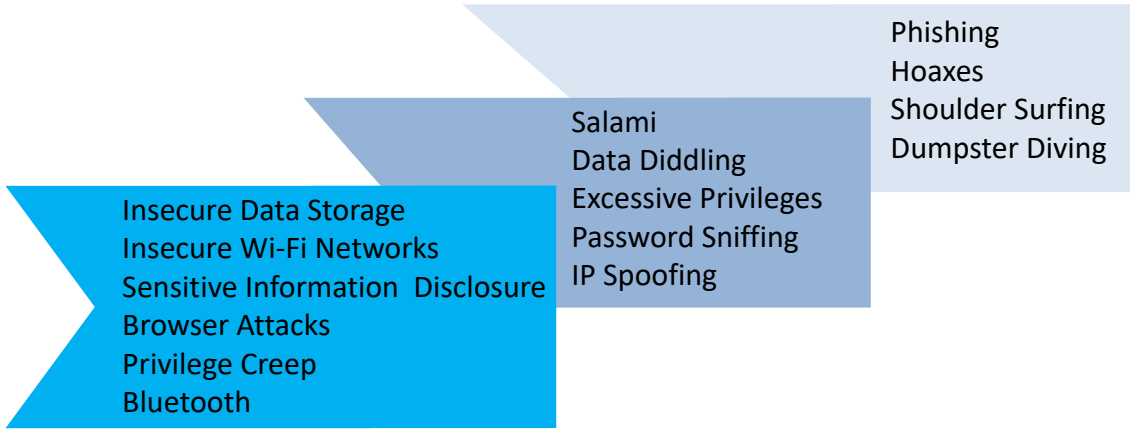
- Performance monitor
- Systems monitor
- Performance baseline
- Protocol analyzers
- Vulnerability Scanning Regiment
- Continuous Diagnostics and Mitigation (CDM)



### External Actions

- Third party auditors
- Penetration tests

# Penetration Testers' Arsenal



# Risk Responses

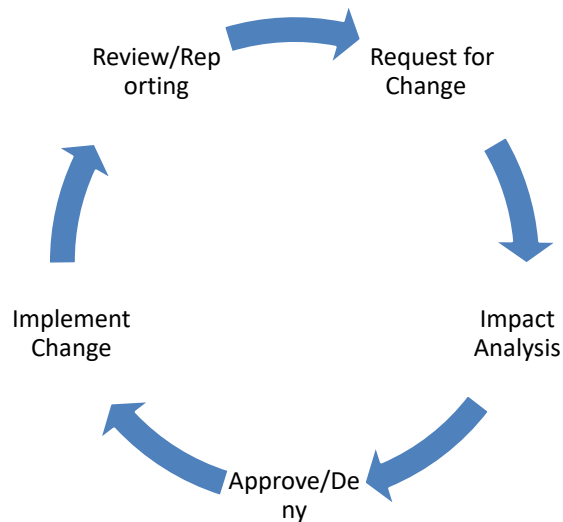


Action	Example
Avoid	Isolate the system, block the service or port
Transference	Insurance or use a third party
Acceptance	System owner and/or executive owner assumes responsibility
Mitigation	Compensating controls and Plan of Action and Milestone (POA&M)





## Mitigation Leads to Change Management



### Critical elements:

- What is the change (software, hardware, firewall...)
- What is the impact on landscape
- Clear procedures to make request and validate the change



33

33

## Forensics



- Investigations
- Chain of custody
- Forensics
  - Legal Hold
- Incident Response
  - Event
  - Incident
- Durability



34

34

# Chain of Custody

Chain of Custody – documentation of who handled or had access to the data (who, what, where (obtained and stored), when (timestamps and the use of ntp on electronic data) and how

Order of Volatility for Electronic Discovery

- CPU, cache, and register contents
- Routing Tables, ARP cache, process tables, and kernel statistics
- Live network connections and data flows
- Memory (RAM)
- Temporary file system/swap space
- Data on hard disk
- Remotely logged data
- Data stored on archival media/backups



35

35

# Evidence

Standards	
Sufficient	Without question
Competent	Legally qualified and reliable
Relevant	Material to the case

Types	
Direct	Specific fact
Real	Associative or physical evidence (tangible objects that proves or disproves a fact)
Documentary	Business records, printouts, manuals
Demonstrative	Models, experiments, and charts



36

36

# Surveillance, Search, and Seizure

Physical surveillance  
Computer surveillance



Evidence Rules	
Best evidence	original (no intentional/unintentional alteration)
Exclusionary	no violation of Fourth Amendment - policies must be in place and acknowledged
Hearsay	second-hand evidence (computer generated data is considered hearsay because the computer cannot be interrogated)



37

37

# Incident Response



Step	Description
Preparation	Establishes the foundation - train employees on roles and responsibilities, drill scenarios, review plan yearly
Detection	Process to determine if breached - when did it occur, how was it discovered, who discovered, impact to landscape, scope, and source
Containment	Contain impacted area
Eradication	Mitigation phase which analyzes the incident including determining the root cause. Final step is to prevent the future impact
Recovery	Return to normal operations
Lesson Learned	Document



Image courtesy of: <https://blog.e-janco.com/2012/08/09/feds-issue-a-computer-security-incident-handling-guide/>

38

38

# Business Continuity

Contingency Plan Test  
 ➤ Tabletop

Recovery Site

Cold	No hardware, no data, no employees
Warm	Limited setup, empty rack space, no data
Hot	Replica or operational setup, hardware and applications replicated and up to date



Failover Site

- Prepare recovery site
- Disaster is declared
- Address disaster
- Return to normal operations site



# Business Continuity Backup Strategies

Type	Data Selection	Archive Attribute
Full	All data	Cleared
Differential	Contains all combined file changes since the last full backup	Not cleared
Incremental	Contains all the changed files since the last backup (no matter which level)	Cleared

Backup Type	Backup Time	Restore Time	Storage Space
Full	Slowest	Fast	High
Differential	Moderate	Fast	Moderate
Incremental	Fast	Moderate	Lowest



# Network



- Storage Area Network (SAN)
- Clustering
- Grid computing
- Backups
- Hierarchical Storage Management (HSM)

## Different RAID Levels

RAID Level	Activity	Name
0	Data striped over several drives. No redundancy or parity is involved. If one volume fails, the entire volume can be unusable. It is used for performance only.	Striping
1	Mirroring of drives. Data are written to two drives at once. If one drive fails, the other drive has the exact same data available.	Mirroring
2	Data striping over all drives at the bit level. Parity data are created with a hamming code, which identifies any errors. This level specifies that up to 39 disks can be used: 32 for storage and 7 for error recovery data. This is not used in production today.	Hamming code parity
3	Data striping over all drives and parity data held on one drive. If a drive fails, it can be reconstructed from the parity drive.	Byte-level parity
4	Same as level 3, except parity is created at the block level instead of the byte level.	Block-level parity

## Different RAID Levels

RAID Level	Activity	Name
5	Data are written in disk sector units to all drives. Parity is written to all drives also, which ensures there is no single point of failure.	Interleave parity
6	Similar to level 5 but with added fault tolerance, which is a second set of parity data written to all drives.	Second parity data (or double parity)
10	Data are simultaneously mirrored and striped across several drives and can support multiple drive failures.	Striping and mirroring



43

43

## Data Destruction and Media Sanitization

Means of Mass Destruction	Description
Burning	Gold standard for data destruction - even SSD
Shredding	Documents and large industrial for hardware
Pulping	For paper fibers are recombined to form new paper
Pulverizing	Physical process using excessive force to destroy hardware
Degaussing	Realigns magnetic particles
Purging	Permanently erase and remove data from a storage device to allow reuse
Wiping	Rewriting with a pattern of 1s and 0s



44

44