DSci526:
Secure Systems Administration

Incident Response Planning

Prof. Clifford Neuman

Lecture 8
10 March 2021
Online

MID-TERM EXAM

MID TERM EXAM IN PROGRESS

Lecture Will Resume
At
4PM Pacific Time

Today's Presentations

Incident Response Planning

- Announcements/Logistics (approx. 5 minutes)
- Incident Response Planning (approx. 35 min)
  - Dr. Neuman's summary of the topic
- Group Project Discussion (40 min)

March 17th – Secure Networking

- Christopher Samayoa (Network Access Control)
- Shanice Williams – Network Monitoring – WireShark
- Pratyush Prakhar – Web Penetration Tools

Presentations March 24th Configuration Management

- Marco Gomez
- Louis Uuh

March 31st – Security Incident Event Management

- Malavika Prabhakar
- Anthony Cassar
- Dwayne Robinson (Network Perimeter Detection)
- MaryLiza Walker (Attack Forensics)
- Jason Ghetian

Linux Related Topics – April 14th

- Azzam Alsaeed – SELinux
- Alejandro Najera – Linux Administration
- Tejas Pandey – Identity Management in Linux
- Ayush Ambastha – Linux Kernel Security

DSci526:
Secure Systems Administration

Incident Response Planning

Prof. Clifford Neuman

Lecture 8
10 March 2021
Online

Response Planning

What are you responding to?

- All failures, security or reliability
- Some parts of the plan will be similar
- Other parts will depend on the nature of the failure

We start with Disaster Recovery

Then we move onto intrusion response

Disaster Recovery Planning

vs Business Continuity Plan (BCP)

- Terminology
- How to write an IT DR Plan
- Backup Strategies
- Replication Technologies

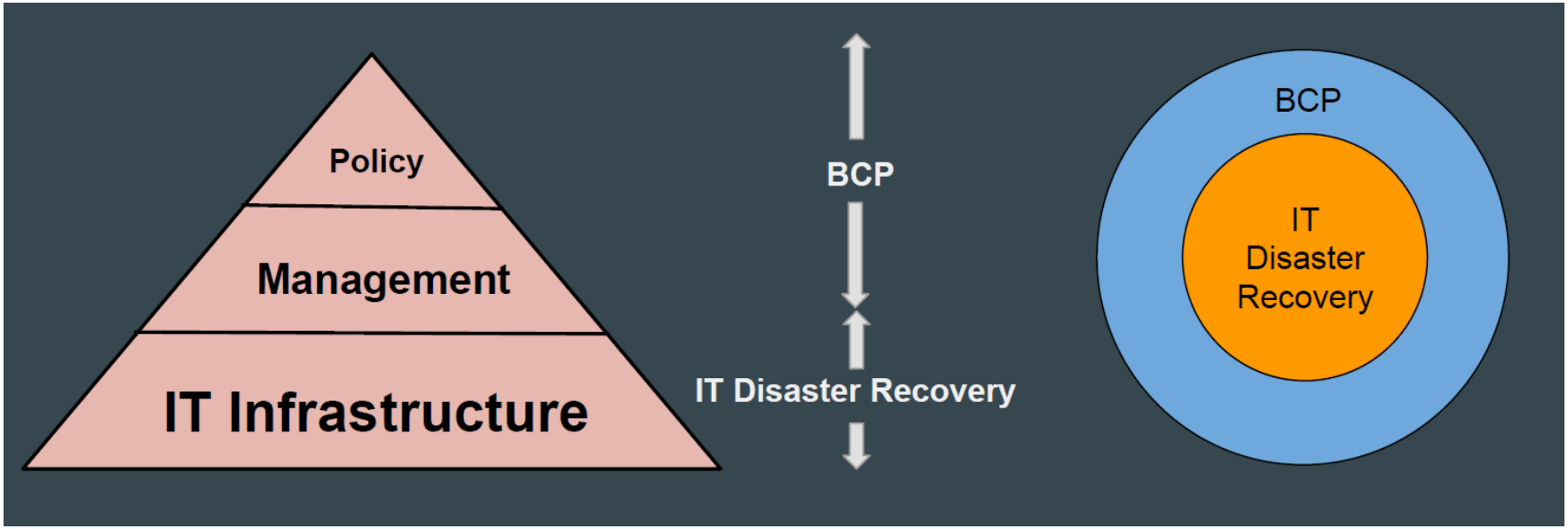
Business Continuity Plan

- The processes and procedures that ensure essential business functions continue to operate during and after a disaster.
- Enables an organization to re-establish services to a fully functional level as quickly and smoothly as possible.
- BCP often covers Non-IT aspects of business, but often extends into IT.
- Includes identification of the resources that are needed to maintain business continuity, such as:
  - Critical personnel
  - Key business processes
  - Recovery of vital records
  - Critical suppliers' identification
  - Contacts of key vendors and clients.
  - Standby Equipment
  - Legal Help
  - Financials
  - Alternate infrastructure

IT Disaster Recovery Plan

- A plan that provides a structured approach for responding to unplanned incidents that threaten an IT infrastructure:
  - hardware,
  - software,
  - networks,
  - processes
  - people.
- Protects organization's investment in its technology infrastructure
- Protects the organization's ability to conduct business

Disaster Recovery vs Business Continuity



Metrics for Objectives

1. Recovery Point Objective (RPO) - The interval of time that might pass during a disruption before the quantity of data lost during that period, exceeds the BCP's maximum allowable threshold or 'tolerance'.
2. Recovery Time Objective (RTO) - The duration of time and a service level within which a business process must be restored after a disaster in order to avoid unacceptable consequences associated with a break in continuity.

How to Write a DR Plan

0. Select the teams and determine responsibility		
1.	Risk identification	Risk register and matrix
2.	Assess vulnerability to those risks	Business impact analysis (BIA)
3.	Determine impact on the business	Business impact analysis (BIA)
4.	Identify critical business functions / IT services	Service catalogue and technology dependency mapping
5.	Design and implement mitigation strategies	Putting the capability in place
6.	Agree activation plans	Writing the runbook
7.	Testing	Agree testing, documentation and KPIs
8.	Ongoing changes and maintenance	Keeping the DR plan up to date

Selecting the Team

- Identification of key personnel and roles.
- Define a non-ambiguous chain of command.
- Determine responsibilities in each role.

Most DR teams are led by the CIO in the ole of Recovery Team Leader. Other roles:

  - Business Continuity/Disaster Recovery planning expert
  - Business unit/operations stakeholders
  - Network and Infrastructure delivery
  - IT systems and services
  - Security Funcions
  - Legal Teams

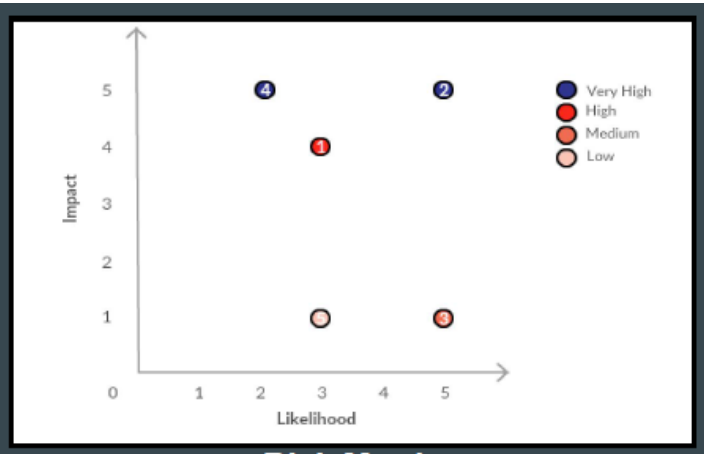
Next Steps

1. Risk Identification
2. Assess Vulnerability
3. Determine Impact

Risk Assessment and Business Impact Analysis

Risk	Likelihood	Impact
DDos Attack	3	4
Earthquake	5	5
Single server failure	5	1
Flooding	2	5
Power failure	3	1

Risk Register

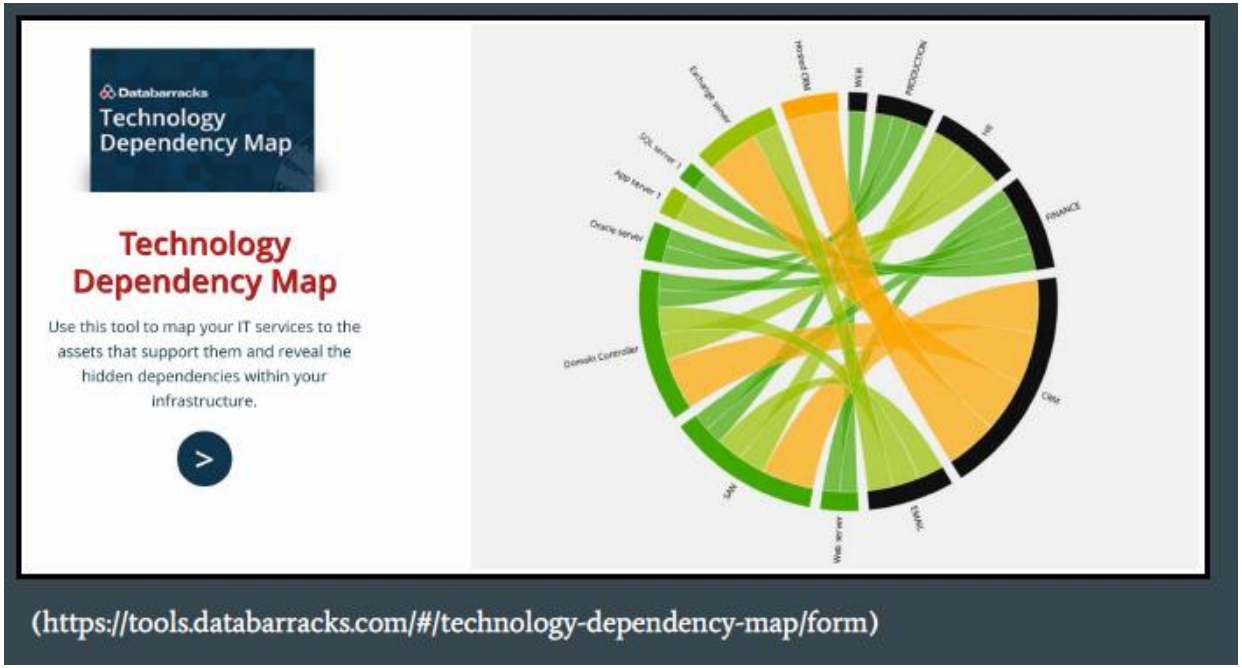


Risk Matrix

(https://tools.databarracks.com/#/risk-register-matrix/form)

4. Identify Critical Business Functions and Services

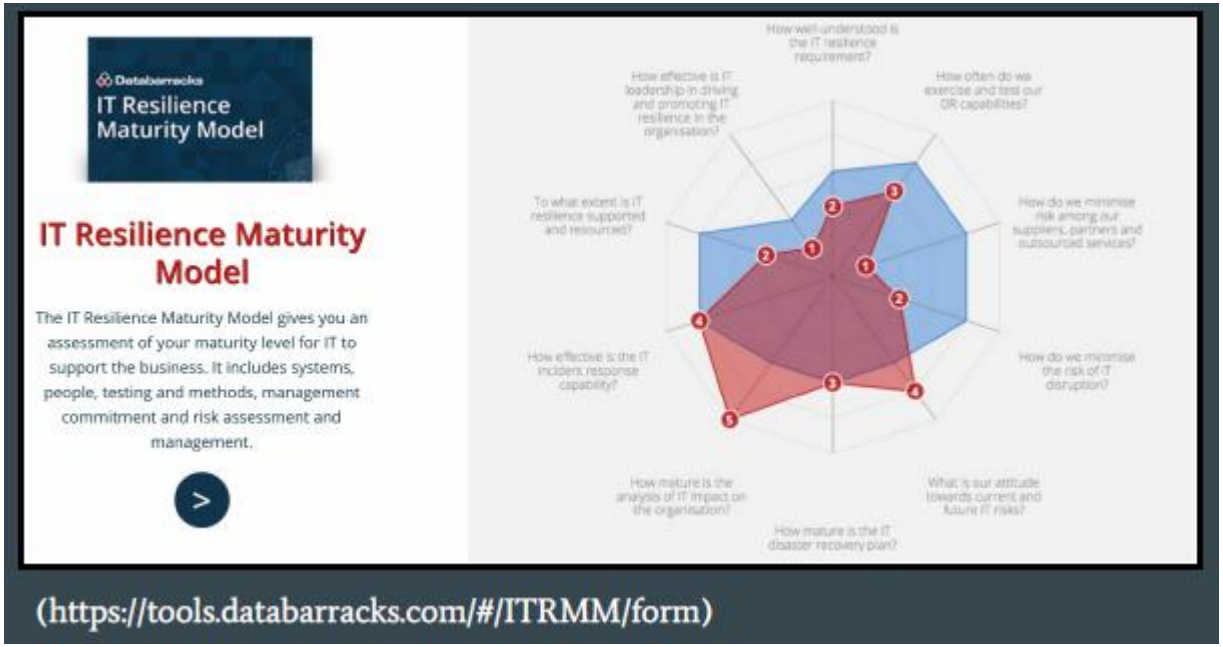
- Definition and analysis of RTOs and RPOs.
- Thinking about services, not IT assets.



- Chord Diagrams
  - Display connection between services and assets
  - Color and Width – Stated Recovery time
    - Thin green – instant
    - Thick orange – a week

5. Design and Implement Mitigation Strategies

- Thinking beyond recovery of services
- Analyzing factors important for restoration:
  - People, facilities, suppliers, replication and backup



- IT Resilience Maturity Model
  - Asks around 10 questions and measures the standard of existing technologies and processes that are plugged into BCP.
  - The tool models the responses on a radial chart.
  - Maturity rating can be compared with a
  - model of responses from peers, SMEs and
  - organizations in highly regulated industries.

6. Agree on Activation Plans

- Generate a runbook, documentation for the plan.
  - For use by management who will take the actions.
  - It should be descriptive and spell out its assumptions

- While stored securely, one should assume others may know what it contains, and this could be used by adversaries. Don't include critical passwords, etc.
- Should spell out who is to be contacted, including any mass notifications.
- Should be specific, get general enough to cover multiple kinds of incidents.
  - E.g. chapters for IT failure, power failure, hacked systems.

7. Testing

- Plan should be tested for efficiency.
- KPIs should be formulated, along with testing strategies and corresponding testplan.
- Metrics should be recorded and analysed for:
  - Test coverage ?
  - Success ?
  - Meeting the recovery objectives ?
- Full disaster recovery test, at least once per year.
- Analysis should be documented..

8. Update and Maintain the Plan

- Your systems change and so must the plan
- If there are changes to the control systems your plan must be updated.
- Schedule a review quarterly to see if any changes require updates to the plan.
- Review teams, activities, and update documentation of plan.

Backups and Replication

- Backups
  - Full Backup - full and complete backup of the entire system.
  - Incremental Backup - only archives data that has been modified that day.
  - Differential Backup - storage of all the files that have changed or been added since last full backup...

Differential vs Incremental

- Differential Backup
  - More files to be backed up, therefore takes more time and uses more storage space.
  - Faster restoration because only the last full backup and the last cumulative backup must be applied.
  - More manageable with lesser number of disks.
- Incremental Backup
  - Fewer files to be backed up, therefore faster backup less storage
  - Restoration takes longer because all the backup disks are used.
  - Difficult to manage and maintain with larger number of disks.
  - High risk of whole chain becoming unrecoverable if any disk corrupted.
  - Testing of backup every time would be costly and time-consuming.
- Incremental may be preferred for cloud backup
  - Less data to transfer, clear recovery points.

Replication

Provides backup process for immediate failover

- Synchronous
  - Writes data to primary and secondary sites at the same time.
  - It's expensive.
  - Introduces latency, slows down the primary site.
  - Preferred for applications with low RTOs (Recovery Time Objectives) that can't abide data loss.
- Asynchronous
  - There's a delay before the data is written to secondary site.
  - Designed to work over distances and use less bandwidth.
  - There is a risk of losing data during an outage.
- Journaling
  - Basically an incremental backup (per transaction)
  - Replayed from journal and last image of system when restarting.

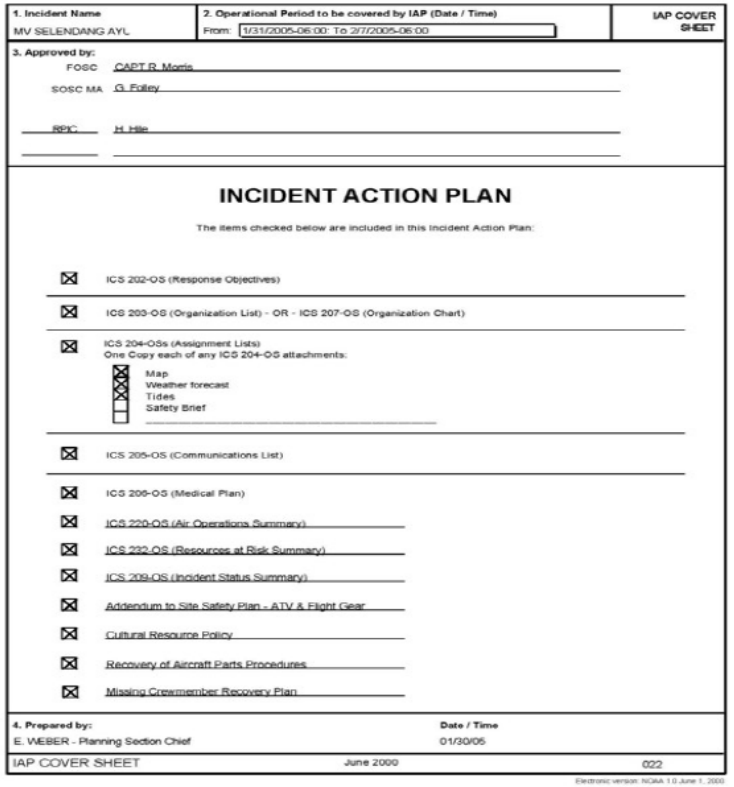
Intrusion Response Planning

What is an intrusion or incident?

- An action likely to lead to grave consequences for your organization.
- Consequences can affect company revenue and business
- Incident examples
  - Virus
  - Malicious code
  - Trojan horse
  - Espionage

Formal Intrusion Response Plan

- Overview
- Purpose
- Incident Response Goals
- Incident Definition
- Incident Planning
- Incident Response Lifecycle



1. Incident Name: MV SELENDANG AYL
2. Operational Period to be covered by IAP (Date / Time): From: 1/31/2005-06:00 To 2/7/2005-06:00
IAP COVER SHEET

3. Approved by:
FOSC CAPT R. Morris
SOSC MA G. Folley
RPIC H. Hile

INCIDENT ACTION PLAN

The items checked below are included in this Incident Action Plan:

- ☒ ICS 202-OS (Response Objectives)
- ☒ ICS 203-OS (Organization List) - OR - ICS 207-OS (Organization Chart)
- ☒ ICS 204-OSs (Assignment Lists)
  One Copy each of any ICS 204-OS attachments:
  - ☒ Map
  - ☒ Weather forecast
  - ☒ Tides
  - ☐ Safety Brief
- ☒ ICS 205-OS (Communications List)
- ☒ ICS 206-OS (Medical Plan)
- ☒ ICS 220-OS (Air Operations Summary)
- ☒ ICS 232-OS (Resources at Risk Summary)
- ☒ ICS 209-OS (Incident Status Summary)
- ☒ Addendum to Site Safety Plan - ATV & Flight Gear
- ☒ Cultural Resource Policy
- ☒ Recovery of Aircraft Parts Procedures
- ☒ Missing Crewmember Recovery Plan

4. Prepared by: E. WEBER - Planning Section Chief
Date / Time: 01/30/05

IAP COVER SHEET June 2000 022

Electronic version: NOAA 1.0 June 1, 2000

Overview, Purpose, Goals, Defintion

- The incident response plan defines what constitutes a security incident and outlines the incident response phases. how information is passed to the appropriate personnel, assessment of the incident, minimizing damage and response strategy, documentation, and preservation of evidence
- The policy is designed to protect the organizational resources against intrusion.
- Incident Response Goals:
  - Verify that an incident occurred.
  - Maintain or Restore Business Continuity.
  - Reduce the incident impact.
  - Determine how the attack was done if the incident happened.

Potential Examples Incident Definition

- Loss of information confidentiality (data theft)
- Compromise of information integrity (unauthorized modification).
- Theft of physical IT asset including computers, storage devices.
- Damage to physical IT assets.
- Denial of service.
- Misuse of services, information, or assets.
- Subversion of systems (Virus, Worms, Ransomware)
- An attempt at unauthorized access.
- Unauthorized changes to hardware, software, or configuration.
- Reports of unusual system behavior.
- Responses to intrusion detection alarms.

Incident Response Planning

- Define roles and responsibilities
- Establish procedures detailing actions taken during the incident.
  - Detail actions based on type of incident such as a virus, hacker intrusion, data theft, system destruction.
  - Procedures should consider how critical the threatened system or data is.
  - **Consider whether the incident is ongoing or done.**

Preparation

- Policies and Procedures
  - Computer Security Policies -These involve many policies including password policies, intrusion detection, computer property control, data assessment, and others.
  - Incident Response Procedures
  - Backup and Recovery Procedures
- Implement policies with security tools including firewalls, intrusion detection systems, and other required items.
- Post warning banners against unauthorized use at system points of access.
- Establish Response Guidelines by considering and discussing possible scenarios.
- Train users about computer security and train IT staff in handling security situations and recognizing intrusions.
- Establish Contacts -Incident response team member contact information should be readily available. An emergency contact procedure should be established. There should be one contact list with names listed by contact priority.
- Test the process.

Detection Analysis

- Analysis and Assessment -Many factors will determine the proper response including: Is the incident real or perceived?
- Is the incident still in progress?
- What data or property is threatened and how critical is it?
- What is the impact on the business should the attack succeed? Minimal, serious, or critical?
- What system or systems are targeted, where are they located physically and on the network?
- Is the incident inside the trusted network?

Recovery

- Restore affected systems to their original state. Be sure to preserve evidence against the intruder by backing up logs or possibly the entire system. Depending on the situation, restoring the system could include one or more of the following re-install the affected system(s) from scratch and restore data from backups if necessary. Be sure to preserve evidence against the intruder by backing up logs or possibly the entire system.
- Make users change passwords if passwords may have been sniffed.
- Be sure the system has been hardened by turning off or uninstalling unused services.
- Be sure the system is fully patched.
- Be sure real time virus protection and intrusion detection is running.
- Be sure the system is logging the correct items

Recovery (2)

- Documentation -Document what was discovered about the incident including how it occurred, where the attack came from, the response, whether the response was effective.
- Evidence Preservation -Make copies of logs, email, and other documentable communication. Keep lists of witnesses.
- Notifying proper external agencies -Notify the police if prosecution of the intruder is possible.
- Assess damage and cost -Assess the damage to the organization and estimate both the damage cost and the cost of the containment efforts.

Post Incident

- Review response and update policies -Plan and take preventative steps so the intrusion can't happen again. Consider whether an additional policy could have prevented the intrusion.
- Consider whether a procedure or policy was not followed which allowed the intrusion, then consider what could be changed to be sure the procedure or policy is followed in the future.
- Was the incident response appropriate? How could it be improved?
- Was every appropriate party informed in a timely manner?
- Were the incident response procedures detailed and cover the entire situation? How can they be improved?
- Have changes been made to prevent a re-infection of the current infection? Are all systems patched, systems locked down, passwords changed, anti-virus updated, email policies set, etc.?
- Have changes been made to prevent a new and similar infection?
- Should any security policies be updated?
- What lessons have been learned from this experience?

Prioritization

- To help prioritize the timing and resources needed to deploy corrective action, resource proprietors and resource custodians must assess the impact of a security incident based on the following factors:
- How the incident will impact existing functionality of the affected systems
- Whether the incident breaches the confidentiality or integrity of covered data (Protection Level 2) or non-covered data
- How much of the user population is affected by the security incident
- What's the reputational/financial impact to organization

Example – Berkeley IR Plan

Incident Response Phases	High Priority Incident	Low Priority Incident
Detection	Immediate	8 hours
Analysis	Resource Manager and incident handler assigned to work with ISP Analyst* on dedicated, continuous basis.	Incident handler assigned and dedicated to work with ISP Analyst on case during normal business hours.
Recovery	Resource Manager and incident handler assigned to work with ISP Analyst* on dedicated, continuous basis.	Incident handler assigned to work with ISP Analyst on case as time/resources are available.
Post-Incident	Incident handler assigned to work with ISP Analyst on case as time/resources are available.	Incident handler assigned to work with ISP Analyst on case as time/resources are available.

Tools for Incident Response

- Digital forensic workstations21 and/or backup devices to create disk images, preserve log files, and save other relevant incident data
- Laptops for activities such as analyzing data, sniffing packets, and writing reports
- Spare workstations, servers, and networking equipment, or the virtualized equivalents, which may be used for many purposes, such as restoring backups and trying out malware
- Blank removable media
- Portable printer to print copies of log files and other evidence from non-networked systems
- Packet sniffers and protocol analyzers to capture and analyze network traffic
- Digital forensic software to analyze disk images
- Removable media with trusted versions of programs to be used to gather evidence from systems
- Evidence gathering accessories, including hard-bound notebooks, digital cameras, audio recorders, chain of custody forms, evidence storage bags and tags, and evidence tape, to preserve evidence for possible legal actions

Additional Tools

- One of the most important resources required for incident response, are system logs. Logs are normally kept individually in each network device. Products such as netForensics, Contegoor ArcSight, may be considered for this process

- Another important tool to consider is computer forensics and security software. When an incident is suspected, forensics software allows you to take a snapshot of a system, capturing and preserving live data, such as, local data storage, open ports, system registry and a RAM dump. Tools involved in this are Encase Enterprise , acessdata FTK etc.

Industry Response Plans

Education:

UCSD - http://blink.ucsd.edu/technology/security/CIRT/index.html

Berkeley - https://security.berkeley.edu/incident-response-planning-guideline

USC Payment related - https://policy.usc.edu/files/2015/05/Appendix-C-PCI-Incident-Response-Plan.pdf

Financial

SANS Guidelines - https://www.giac.org/paper/gsec/3902/incident-response-planning-smaller-financial-institutions/106243

VISA - http://www.aicpa.org/interestareas/informationtechnology/resources/privacy/downloadabledocuments/incidentresponse.doc

AICPA - http://www.aicpa.org/interestareas/informationtechnology/resources/privacy/downloadabledocuments/incidentresponse.doc

DSci526:
Secure Systems Administration

First Group Project
(second week reports)

Prof. Clifford Neuman

Lecture 8
10 March 2021
Online

Teams for First Group Project

- Team One
  - Shagun Bhatia
  - Anthony Cassar
  - Sarahzin Chowdhury
  - Aditya Goindi
  - Tejas Kumar Pandey
  - Malavika Prabhakar
  - Pratyush Prakhar
  - Dwayne Robinson
  - Christopher Samayoa
  - Amarbir Singh
  - Louis Uuh
  - Shanice Williams
- Team Two
  - Azzam Alsaeed
  - Ayush Ambastha
  - Jason Ghetian
  - Marco Gomez
  - Alejandro Najera
  - Doug Platt
  - Abhishek Tatti
  - Carol Varkey
  - MaryLiza Walker
  - Yang Xue
  - Hanzhou Zhang

Banking Scenario

- Your organization must:
  - Maintain a database of account holders
  - A database of account balances
  - Enable web access by customers who:
    - Can update their personal information
    - Check their account balance
    - Transfer funds to another account (by number)
    - View transactions on their account
    - Submit an image of a check for deposit
      - (check should be viewable, but you do not need to scan it or process it)
- Access is needed
  - Via web from the open internet
  - Outbound email confirming transactions
  - All other interactions may be limited by information flow policies to internal machines.

Reports from Both Teams

- 1640-1650 Group One Reporting
- 1650-1700 Group Two Reporting
- 1700-1720 Open Discussion among class
- then Breakout Rooms for Groups