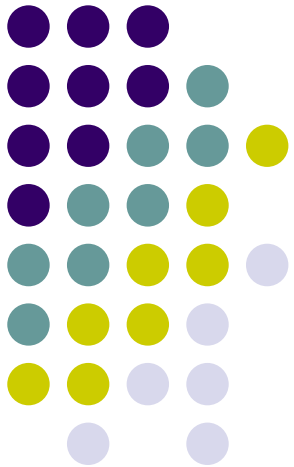
3.05 - Case Study
Security BCP Tsunami Simulation

Fourteenth National HIPAA Summit

March 29, 2007



Mike Walder, CISSP
Secure Technology, Inc.

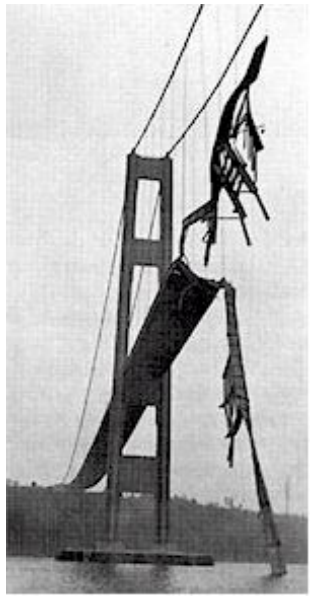
SECURE TECHNOLOGY HAWAII

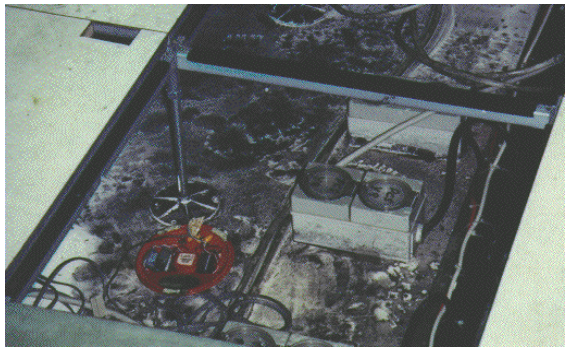
Why Bother?

Why should we worry about disaster recovery for computer and network systems?

- Some of my favorite excuses:
  - I am too busy to worry about this right now!
  - Yeah, but the chance of it happening is so small…
  - I bought really expensive HP computers…
  - My IT team makes backups all the time…
  - We can live without our computer systems for at least week
  - Well, if it ever happens, then we will can get a budget…

When Disasters Attack!

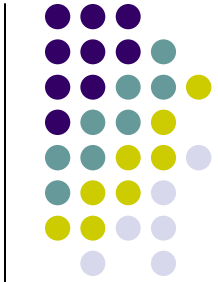




My Top 6 Disaster Experiences

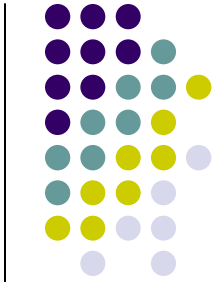
- Chicken Pox 1 day before my first day at work on a new job
- Broken sprinkler dumps water on core MicroVax 3 hours before DoD acceptance test
- SW developer Didn't backup disk and lost 4 months of assy code
- Engineer's gold chain shorted out custom circuit board costing project 3 month delay and a new board worth about $100k
- At age 5 clearing the snow off my dad's new car with a shovel
- Not remembering to do what my wife told me

Agenda



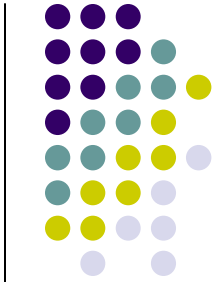
- Project Background
- Purpose of the Simulation
- What IT did
- What Operations did
- Benefits
- Recommendations

Project Background



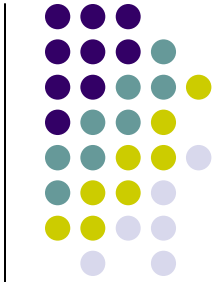
- State of Hawaii, DHS
- Multi-Year, Multi-Phase Compliance Project
  - Security Assessment
  - Privacy Training
  - Remediation Planning & Execution
  - Business Impact Analysis (BIA)
  - Business Continuity Planning
  - Contingency Plan Training & Simulation
  - Follow on Assessment

Objectives



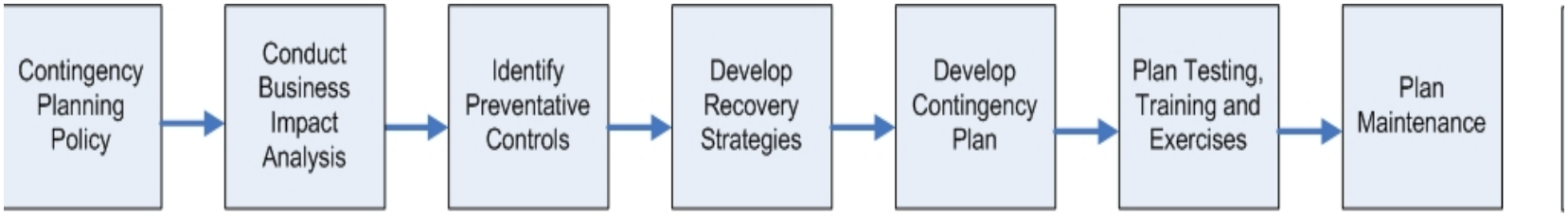
- BCP Purpose
  - To document operational plans and procedures to be followed in emergencies, system disruptions or disasters in order to continue critical business and IT operations
- DHS Mission Statement
  - Continue essential business and IT operations in emergency mode
  - Provide emergency assistance as required by Hawaii State disaster plans
  - Recover normal business operations after the emergency or disruption
  - Recover normal IT functions after the emergency or disruption
  - Recover critical data and system assets that would otherwise be lost as a result of the emergency, disruption, or disaster
- Hawaii Civil Defense / COOP

Org, Network & Apps



- Multiple offices throughout the State
  - Two Internet Connections, large WAN
- Primary Mainframe applications
  - Hawaii and on Mainland
- Other applications
  - Email
  - Custom databases
  - Emulators
  - Network access / file servers

By the book process



- Identify Regulatory Requirements For Contingency Plans
- Develop IT Contingency planning policy statement
- Obtain approval of policy
- Publish policy

- Identify IT resources
- Identify business processes
- Identify outage impacts and allowable outage times
- Develop recovery profiles

- Implement controls
- Maintain controls

- Identify methods
- Integrate information system architecture

- Document recovery strategy

- Develop test objectives
- Develop success criteria
- Document lessons learned
- Incorporate into the plan
- Train personnel

- Review and update plan
- Coordinate with internal / external organizations
- Control distribution
- Document changes

Business Impact Analysis

- Identified & classified the threat(s)
  - Natural, man-made, terrorist, cyber
- Assessed the risk to DHS
  - Loss of life, data, money, productivity
- Identified business critical activities
  - Payment processing, email,
  - Acceptable downtime ranged from 24 - 72 hours
- Determined support staffing needs
  - Management, business Units, IT

Developed Recovery Plan

- Addressed the BIA results
- What we found
  - Some recovery is centralized
    - Customer information, printing, storage
  - Some recovery is distributed
    - Staff may need to work from anywhere
    - PC's, phone, remote networks
- We looked at the recovery approach first and then fine tuned the backup method
- Communications were still the key

Threat Severity & Consequences

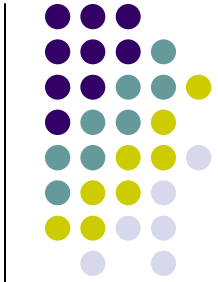
Loss Type Time	1-3 Days	4-7 Days	8 or more days	
Loss of access	1	2	3	
Loss of core data	2	2	3	
Loss of access and core data	3	3	3	
Loss of Access and Core Data with activation of Civil Defense		4	4	4

- Threat Consequences
  - Loss of personnel
  - Loss of vital business records
  - Loss of voice communications
  - Breach of computer security
  - Loss of access to mission critical computer systems
  - Loss of access to buildings
- Lingering Effects

Purpose of the Simulation

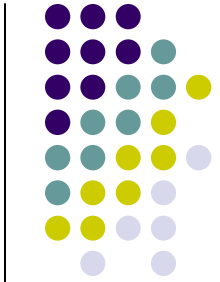
- Gain an understanding of the business contingency planning process and operations
- Train staff on preventative controls, disaster readiness, interim operation procedures, systems recovery, and post event cleanup
- Initiate the creation of a department-wide interim operations log
- Validate technical recovery procedures
- Prioritize applications and process needed during disasters

Simulation Specifics



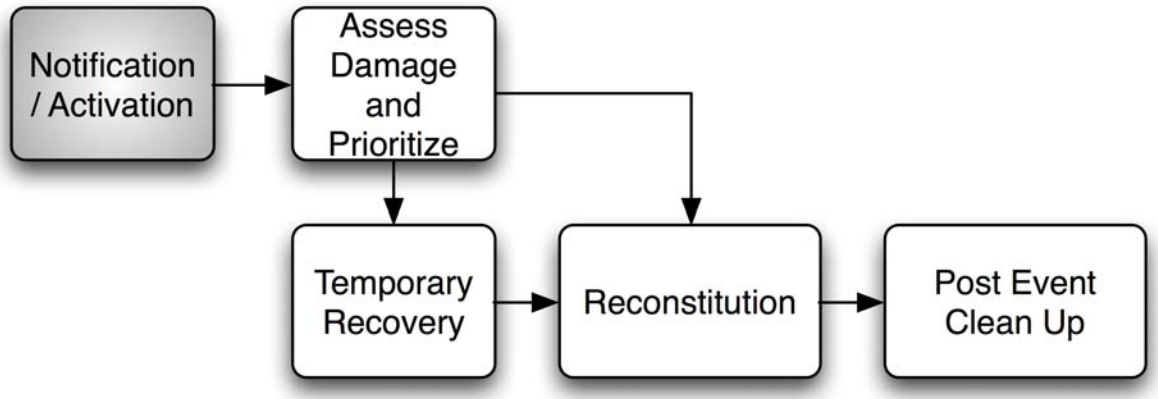
- Severity Level 4
- Tsunami
- Buildings with servers / networks damaged and flooded
- Other locations available
- Limited power & telecom back available in 48 hours
- Loss of access and essential data
- Anticipated 7 days duration

Our Simulation - 4 Days

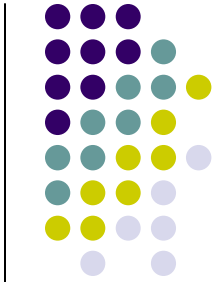


- Day 1 - Group Meeting
  - Emergency Declared
  - High Level Plans Reviewed
- Day 2 - Two Teams - Operations & IT
  - Different locations
  - Operations group broke into teams, went through checklists
  - IT Group validated portable recovery of applications
- Day 3 - Teams still split
  - Operations Group practiced different procedures and actions
  - IT Group discussed different recovery steps & priorities
  - Both sides developed new recommendations
- Day 4 - Group Session To Share Results
  - Team presentations & feedback

Simulation Stages

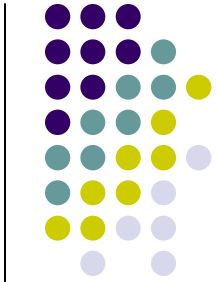


IT Day 2



- Mainframe and network teams
- Met at off site location
- Focused on recovery demonstration
- Started off with recent experiences

Reviewed Earthquake Example



- Real Earthquake happened after simulation test was planned but before it was conducted
- Discussion
  - Event - Earthquake off Big Island
  - Local physical damage
  - Power outage statewide - ranged from 4-36 hours
- Per Division Review
  - What did each Department / Division Do?
  - Were they notified
  - How did they decide disaster was over?
  - Any changes to original plans?

Current backup approach

- Backup of computer systems
  M-F to disk or tape
- Take a copy off site (sometimes)
- Lots of partial backups - journaling
- Effective for simple recovery only
  - Should be able to restore deleted or corrupted files on the same server
  - Team agreed this will FAIL on different hardware
  - Recovery was rarely attempted

Recovery First

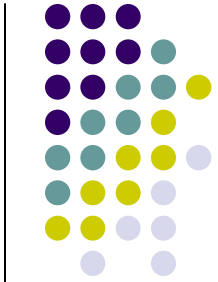
- Recovery must be able to:
  - Restore deleted / corrupted files to the same server
  - Restore the entire system to different hardware
  - Produce a working system in an acceptable timeframe

  - If you cant do these, be prepared to pay the cost of downtime

Reviewed Recovery Strategies

- Data center recovery site
  - Option 1 - Cold site - Portable
  - Option 2 - Hot site
  - Option 3 - Replication fail over site
- Centralized user recovery site
  - IPSEC VPN to data center recovery for data
  - Phone Service, Printing and Supplies
- Decentralized users
  - SSL VPN to data center recovery for data
  - Phone service

Virtualize Servers Using VMWare

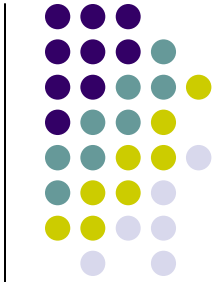


- Mainframes use virtualization
- What is VMWare?
  - Software that loads on PC servers
  - Virtualization for standard PC hardware
  - Works with Windows, Linux & Novell OS
  - Allows several virtual servers to run at the same time on one PC system
  - Image can be easily moved from one PC system to another without reloading

Virtual Server Efficiency

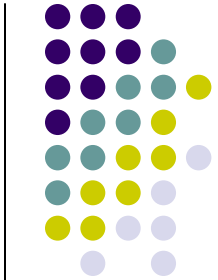
- Virtual servers allow for snapshots for testing of patches and recovery
- Virtual server images can be moved between hardware systems by simple drag-and-drop
- With centralized storage, virtual servers can be moved while applications are running live.

STHI Portable Recovery Kit



- VMWare environment runs on most PC servers
- Secure remote access for non-tech staff
- Combine Key Functions in VM
  - SSL, TS / Citrix, Directory are integrated
  - Email, File Server, Emulators, Key Applications
- Email and normal logins will work
- Can load other key applications
- Anywhere, anytime, from any PC

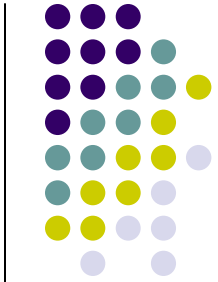
How STHI Portable Recovery Works



- *With a DVD and a USB drive, you can recover a business*
- *Create an environment that will work on any VM Server*

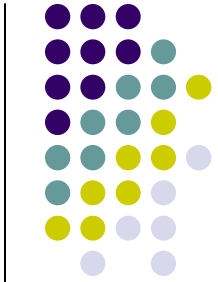
- Dedicated server for DR - VM ESX to build image
- VM Images
  - SSL Portal (Checkpoint)
  - Backup domain controller / directory (A/D)
  - Email Server (Exchange or Lotus) in dial tone mode
  - Terminal Services or Citrix
  - Key Applications & data (Restore or P-V Convert)
- Take Snapshot Image & Compress
  - Look at each app for how best to snapshot
- Develop Bootstrap Loader
  - DVD to create first VM, provided de-compression

Operations Day 2



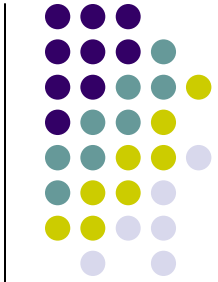
- Met at offsite location
- Representatives from most Divisions
- Broke up into small teams
  - Defined purpose
  - Identified needs

Stages of Recovery



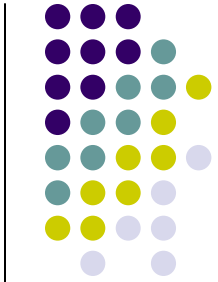
- Went through stages of contingency planning
  - Data backup
  - Assets criticality analysis
  - Emergency supplies lists
  - Staff lists and roles
  - Training
  - Testing and updates
- Notification /Communication – Contact Trees
- Interim Operations – Checklists

Operations Day 3



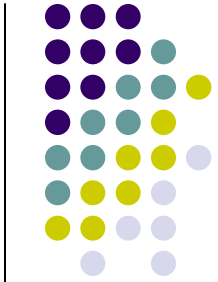
- Met at offsite location
- Finished recovery and reconstitution
- Transfer alternative sites to normal
- Document activities, Transfer paper records
- Establish normal communications
- Finalize and document all checklists, contact trees
- Prepare presentation to large group

Operations Findings



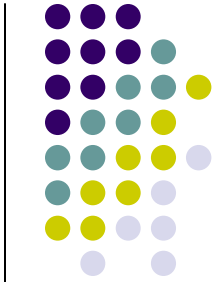
- It was really eye-opening for the non-technical teams to think through what recovery really meant
- Importance of clear purpose for each Division in the emergency
- Define one group as communications hub
- Second group is alternative communications
- Key requirement is to verify eligibility of the client
- Might need to use alternative systems to do this.
- Divisions are meeting to improve upon process and forms

IT Day 3



- Mainframe and network teams
- Met at off site location
- Focused process and feedback

After Personal Safety Was Established

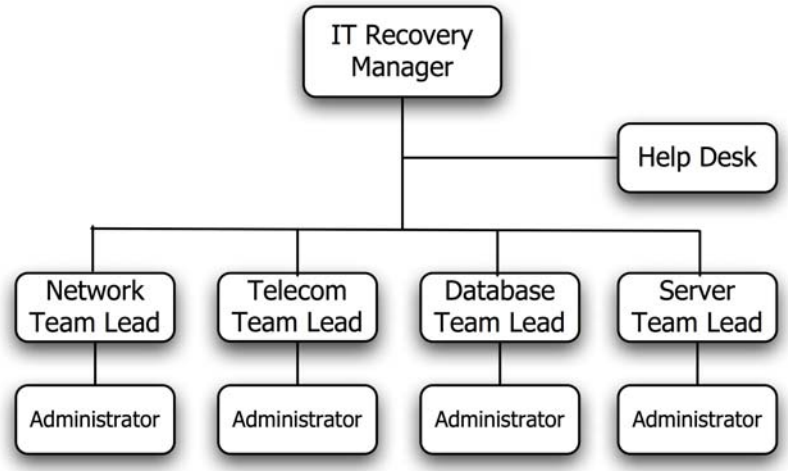


- Emergency response engaged
- Assess the damage
  - Group leaders
  - Environmental
    - Structural, safety, access
  - Technical
    - Power, cooling
    - Transport, network and gateways
    - Remote service providers
    - Application servers
    - Backup media / recovery systems

Checklists & Call Trees

- Checklists
  - Used for all impacted procedures
  - Created new ones when operations changed

- Call Trees
  - Administrative
    - Per Division / Department
  - Technical
    - Network Down
    - Mainframe Down



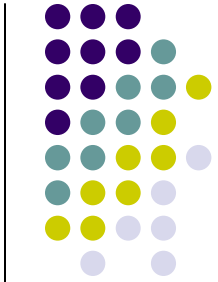
Followed Triage Approach

- Contingency Triage Process
  - Failure Types / Repair Procedures / Time
    - Core & Edge Routers
    - Firewalls
    - Application Servers
    - File and Print Servers
    - Infrastructure
      - DNS, DHCP, Directories
    - Workstations
    - Transports
      - Internet, Wan, etc

Contingency Assessment Matrix

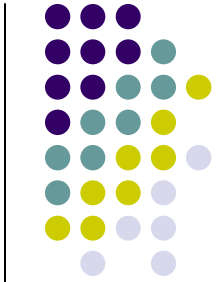
ITEM	FAILURE TYPE	CONTINGENCY	CONTINGENCY EXECUTION TIME	STANDARD REPAIR PROCEDURE	STANDARD REPAIR TIME
Internet network connection	Complete loss of signal	Reroute all traffic through alternate internet feed(s) if available	Approximately 1-4 hours	Wait for connectivity to be restored	1-2 hours average, but if outage exceeds 1-2 hours, estimate increases to 1-3 days
	Loss of IP routability (feed live, no IP traffic routes through to internet)	Reroute all traffic through alternate internet feed(s) if available	Approximately 1-4 hours	Wait for connectivity to be restored	2-4 hours, but if outage exceeds 2-4 hours, estimate increases to 1-3 days
	Known physical disruption of connection (I.e. cable trunks cut or broken)	Reroute all traffic through alternate internet feed(s) if available	Approximately 1-4 hours	Wait for connectivity to be restored	1-3 days

Application Priority



- Mainframe Applications
- Mainframe Gateway
- Domain and Backup Domain Controllers
- Email Servers
- Anti-Virus Management Servers
- Backup Servers
- Database Servers
- File and Print Servers
- Authentication Server
- Network Management and Deployment Servers
- Test and Development Servers

Communications & Documentation

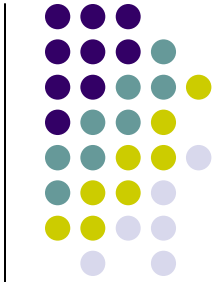


- Assigned technical liaison for each area
  - Documented status and provided buffer
  - Got directives from Recovery Management
- Documentation
  - Discussed - How do they want to do this?
  - Discussed - What should be documented?
  - Discussed - How should info be captured?
- Share Information
  - Get update from Recovery Management on what is priority, situational state, timing, etc.
  - Prepared IT recovery plan

Day 4 – Group Meeting

- Lessons Learned & Benefits

IT Team Set New Goals

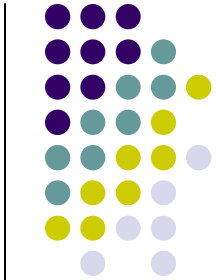


- Network
  - Redundancy at important junction points
  - Spares located at different facility
  - Redundant transport
  - Copies of all router configurations captured & offsite
- Connections to the Internet
  - Redundant ISP at each FW location
    - Local services in limited HA mode
      - Service Specific
  - Cooperative ISP redundancy
    - Two locations, each with ISP connection
    - Failover ISP to each
    - BGP and OSPF might be difficult to build and maintain
- ID / Naming / Directory
  - Redundant DNS, DHCP, Directories

Tests Developed

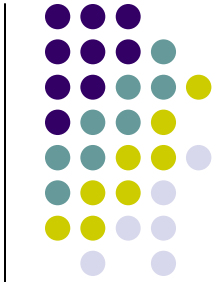
- Local LAN
  - Managed Switches - What info does this provide?
  - What does a defective switch look like?
  - Did they have sniffer and know how to use it?
  - Visual vs connectivity
- DHS WAN
  - Frame Relay connections
  - What do Frame errors look like?
  - Numbers and ID's to call transport vendor?
  - Hopping from router interface to isolate
  - Subnet diagram - highlight what is working and not.
- WAN to Mainframe Applications
  - What does good traffic looks like?
  - What can be done to debug this?

Paper Versions Are Important



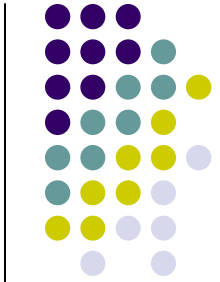
- Paper versions of configurations
  - Server operating system standards
  - Desktop operating system standards
  - Switch and router configurations
  - Firewall configurations
- Support contact information from key vendors
  - Service level agreements
  - Support contracts
  - Phone numbers and email addresses
- Diagrams of all DHS Networks at the subnet level
- Computer equipment inventories
- Policies & Procedures

IT Records Are Important



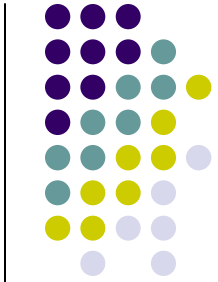
- Software License Keys and Software Images for key systems
  - Operating Systems for servers and desktops
  - Switch & router firmware
  - Firewall firmware and software
  - Other Application & Database systems
  - CD, DCD, or ISO images on Disk Drives
- Support registration information for key vendors

Simulation Summary



- Operations & IT actually talked to each other
  - They now understand each others priorities
  - Established more trust
- Power is really important, but not everything
  - Need to practice what IT can do until power is restored
- Not sure who says the buildings are OK to use
  - Everyone said they would just go into the buildings
  - Those responsible are really understaffed
- Some applications are really important
  - Its really clear now what the priorities are
- Spares are needed for network components
- VMWare provides amazing utility
  - Portable recovery really works
  - Generic hardware
  - VM should be used for production applications too

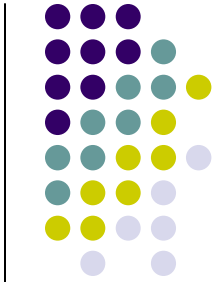
Is Your Organization Ready?



- Recovery solutions drive how things are backed up
- If you don't practice recovery, it probably will not work
- Documentation of key configurations, contracts is off site
- Backups are off site
- Are your BIA, BCP & COOP plans complete and current?
- Have your staff tried to work from an alternative location?

- ***Start simple - Pick 1 or 2 departments***
- ***Make your recovery portable***
- ***Practice, practice, practice!***

Mahalo



- **Secure Technology Hawaii, Inc.**
  - Expert Security and Disaster Recovery Solutions
  - Assessments, Forensics & Simulation Testing
  - PCI Solutions & Managed Services
  - 7x24x365 Comprehensive Technical Support
  - Hawaii, Conus, Pacific Rim

    - Mike Walder, CISSP, President
      mwalder@sthi.com, 808.951.5914:101