“...only way to change is through enforcement...”

“...our 5% budget reduction doesn’t change anything...”

“... enforcement revenues will be used for restitution for victims...AND... reinvestment in STRATEGIC ENFORCEMENT...”

“... enforcement will continue and intensify...”

“... we’re moving from complaint-driven to proactive enforcement...”

“... we’re looking for the “whole menu”...get going on training, PnPs and risk analysis...”
Disaster Preparedness Best Practices

Bob Chaput, MA, CISSP, CHP, CHSS
Clearwater Compliance LLC
Bob Chaput
CISSP, MA, CHP, CHSS, MCSE

- President – Clearwater Compliance LLC
- 30+ years in Business, Operations and Technology
- 20+ years in Healthcare
- Executive | Educator | Entrepreneur
- Global Executive: GE, JNJ, HWAY
- Responsible for largest healthcare datasets in world
- Numerous Technical Certifications (MCSE, MCSA, etc)
- Expertise and Focus: Healthcare, Financial Services, Legal

- Member: NMGMA, HIMSS, ISSA, HCCA, ACHE, AHIMA, NTC, ACP, Chambers, Boards

bob.chaput@clearwatercompliance.com | 800-704-3394

http://www.linkedin.com/in/BobChaput
Learning Objectives

- Explain Key Business Continuity Planning (BCP) / Disaster Recovery Planning (DRP) Terms
- Describe The Explicit HIPAA Security Rule Requirement For A Contingency Plan
- Articulate The Project Initiation Steps For BCP And DRP
- Explain The Difference Between A Business Continuity Plan, Disaster Recovery Plan (DRP) And Data Protection Plan (DPP)
- Complete A Sample Business Impact Analysis For Your Business
- Explain Key Planning Parameters Such As Recovery Time Objective, Recovery Point Objective And Data Loss Event
- Describe Backup And Offsite Facilities
- Describe Types Of BRP Drills And Tests
Session Agenda

1. Why Care?
2. Key Terminology
3. HIPAA Regulatory Requirement
4. How to Get Started
5. Specific, Practical Best Practices
6. Business Impact Analysis Exercise
Why Should You Care?

1. It’s the law… HIPAA & HITECH!

2. Your stakeholders trust and expect you to do this

3. Your revenues, assets and reputation depends on it!
Why Bother?

Lost data exposes your business and clients to business disruption and possible legal set backs

Business and client data is more visible and valuable than ever...

and more vulnerable than ever

And, it’s federal regulation !!!

(GLBA, HIPAA, HITECH, SOX, SEC Rule 17a, PCI DSS, FACTA, etc)
93% of companies that experience a significant data loss will be out of business within five years.

Of the companies that lose their data in a disaster, nearly 50% never reopen their doors at all!

7 of 10 SMBs that experience a major data loss go out of business within a year.

(Source: U.S. Department of Labor; University of Texas; DTI/Price Waterhouse Coopers)
FINDING 1: Despite warnings, most SMBs are still not prepared for disaster

Respondents were asked about their company’s state of readiness to deal with an outage or disruption to their computer or technology resources. Only half (50 percent) responded that they already have a plan in place. That’s up slightly from 47 percent last year. Fourteen percent do not have a plan, nor do they have any intention to create one.

There were some differences according to company size. Fifty-seven percent of small businesses don’t have a plan, compared to 47 percent of medium businesses. Of the respondents who do plan to implement a plan in the future, 16 percent plan to do so within 30 days, 34 percent plan to do so between one and three months, and 25 percent plan to do so between three and six months.
FINDING 2:
SMBs are at risk

It is alarming that more SMBs do not have plans to help them deal with disasters and keep their computer systems up and running, especially when one considers that 65 percent of SMBs reside in regions that they consider susceptible to natural disasters.

In fact, SMBs experienced a median of 6 outages in the past year. The top three reasons for downtime include cyberattacks, power outages, employee errors, and upgrades, with each occurring a median of once per company in the last year.

The survey found that SMB information is not protected. Only half of companies surveyed back up at least 60 percent of their data, and less than half back up their data weekly or more frequently. Only 23 percent back up daily.
FINDING 3: SMBs do not act until it is too late

Of SMBs with a disaster preparedness plan, half (50 percent) implemented the plan due to either an outage or data loss. Fifty-two percent put together their plans within the last six months. However, only 28 percent have actually tested their recovery plans, which is a critical component of disaster preparedness.

Again, there were some differences according to company size. Thirty-six percent of small businesses with a disaster preparedness plan implemented their plan within the last six months, compared to 58 percent of medium businesses.
Finding 4: Not being prepared can have a negative impact

Disasters can have a significant financial impact on SMBs. Downtime costs SMBs a median of $12,500 per day. It costs small businesses a median of $3,000 per day and medium businesses a median of $23,000 per day.

Outages also have a considerable effect on SMB customers. SMB customers reported that SMB outages cost them $10,000 per day, and 29 percent said they lost “some” or “a lot of” data as a result of disasters impacting their SMB vendors.

Downtime also causes customers to leave with 54 percent of SMB customer respondents reporting they have switched SMB vendors due to unreliable computing systems, a 12 percent increase compared with last year’s survey.
Session Agenda

1. Why Care?
2. Key Terminology
3. HIPAA Regulatory Requirement
4. How to Get Started
5. Specific, Practical Best Practices
6. Business Impact Analysis Exercise
Key Terminology

- Risk Management
- Risk Analysis
- Threat Sources
- Vulnerabilities
- Risks
- Business Resumption Planning
- Business Continuity Plan

- Disaster Recovery Plan
- Data Backup and Recovery Plan
- Business Impact Analysis
- Recovery Time Objective
- Recovery Point Objective
- Data Loss Event
What is Risk Management?

Risk = Impact * Likelihood

Goal = Understand What Risks Exist and Into What Category They Fall
Risk Analysis

The examination of assets, their threats and vulnerabilities to identify and evaluate risks

... Risk analysis is defining the whole shape of your information security program – make sure you do it right!

...
Threat Sources

1. **Adversarial**
   - Individual- Outsider, -Insider, Group- Ad hoc, -Established...

2. **Accidental**
   - Ordinary User, Privileged User

3. **Structural**
   - IT Equipment, Environmental Controls, Software

4. **Environmental**
   - Natural or man-made disaster (fire, flood, hurricane), Unusual natural event, Infrastructure failure/outage (telecomm, power)

... An adapted definition of threat Source, from NIST SP 800-30, is “The intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally exploit a vulnerability...”
Vulnerabilities

1. Lack of strong password
2. Lack of personal firewall
3. Lack of data backup
4. Lack of policies
5. Failure to follow policies
6. Lack of training
7. Lack of encryption on laptops with ePHI...
8. ...and on and on ...

NIST Special Publication (SP) 800-30 as “[a] flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system’s security policy.”
Threats Trigger Vulnerabilities ➔ Risk

Threat Source
• Natural Disaster

Vulnerabilities
• Backup data stored onsite
• No alternate recovery site
• Lack of BCP/DRP
• Lack of testing / training

Risks
› Financial
› Political
› Legal
› Regulatory
› Operational impact
› Reputational
Business Resumption Planning

Preplanned procedures allow an organization to:

- Provide an immediate and appropriate response to emergency situations
- Protect lives and ensure safety
- **Serve your customers ... again**
- Reduce business impact
- Resume critical business functions
- Work with outside vendors
- Ensure survivability of the business
- **Get “up and running” quickly**
Business Resumption Planning

Business Continuity Plan

Data Backup and Restoration Plan

Disaster Recovery Plan
Business Impact Analysis (BIA)

The BIA is performed at the beginning of business resumption planning to identify the processes that would suffer the greatest financial or operational loss in the event of a disaster or disruption.

How bad is it going to hurt and how long can we deal with this level of pain?
Recovery Time Objective (RTO)

- RTO – Recovery Time Objective
  - A.K.A., Maximum Allowable Downtime or Maximum Tolerable Downtime
  - Estimates the outage time that can be tolerated by the company as a result of various unfortunate events.
  - How fast does the business / process need to be operational again?
- Sample Recovery Time Objectives…

<table>
<thead>
<tr>
<th>RTO</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nonessential</td>
<td>30 days</td>
</tr>
<tr>
<td>Normal</td>
<td>7 days</td>
</tr>
<tr>
<td>Important</td>
<td>72 hours</td>
</tr>
<tr>
<td>Urgent</td>
<td>24 hours</td>
</tr>
<tr>
<td>Critical</td>
<td>Minutes-Hours</td>
</tr>
</tbody>
</table>

[Image of Healthcare Billing & Management Association logo]
Recovery Point Objectives

- RPO – Recovery Point Objective
  - The point in time to which data must be restored to successfully resume processing
  - Back to what point in time is it acceptable to resume / restart / recreate operational activity?
  - OR, said another way, how much data, time, productivity can we afford to lose?

<table>
<thead>
<tr>
<th>Data Loss</th>
<th>Downtime</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Recovery Point Objective)</td>
<td>(Recovery Time Objective)</td>
</tr>
</tbody>
</table>
Data Loss Event (DLE)

- Data Loss Event
  - Not all “events” are created equal
  - Not equal impact
  - Not equal frequency or probability
  - Against which “events” are you going to focus your efforts?
Data Loss Event Pyramid

Against which Data Loss Events are you building your plan?
Session Agenda

1. Why Care?
2. Key Terminology
3. HIPAA Regulatory Requirement
4. How to Get Started
5. Specific, Practical Best Practices
6. Business Impact Analysis Exercise
§ 164.308 Administrative safeguards.

(a)(7)(i) **Standard: Contingency plan.** Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.

(ii) **Implementation specifications ...**
(ii) Implementation specifications:

- (A) Data backup plan (Required). Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.

- (B) Disaster recovery plan (Required). Establish (and implement as needed) procedures to restore any loss of data.

- (C) Emergency mode operation plan (Required). Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.

- (D) Testing and revision procedures (Addressable). Implement procedures for periodic testing and revision of contingency plans.

- (E) Applications and data criticality analysis (Addressable). Assess the relative criticality of specific applications and data in support of other contingency plan components.
New Civil Monetary Penalty System

- **Tier 1 (Accidental)**
  - $100 each violation
  - Up to $25,000 for identical violations, per year

- **Tier 2 (Not Willful Neglect, but Not Accidental)**
  - $1000 each violation
  - Up to $100,000 for identical violations, per year

- **Tier 3 (Willful Neglect, but Corrected)**
  - $10,000 each violation
  - Up to $250,000 for identical violations, per year

- **Tier 4 (Willful Neglect, Not Corrected)**
  - $50,000 each violation
  - Up to $1.5 million, per year
Session Agenda

1. Why Care?
2. Key Terminology
3. HIPAA Regulatory Requirement
4. How to Get Started
5. Specific, Practical Best Practices
6. Business Impact Analysis Exercise
BRP Methodology Overview

**Initiate BRP Program**
- Obtain executive input on risks and critical processes of the organization
- Educate management and stakeholders on BRP program
- Understand the current state of BRP readiness
- Create BRP Project Plan
- Deliver business continuity methodology & technology training

**Conduct Business Impact & Risk Analyses**
- Determine management’s tolerance for downtime
- Assess potential threats to business processes and sites
- Identify / analyze critical business processes and identify process interdependencies
- Facilitate session to obtain risk management decision by management

**Select Recovery Strategies**
- Assess existing recovery strategy that can be leveraged
- Determine a viable recovery solution
- Perform cost/benefit analysis
- Present management recommendations & obtain approval

**Document Plan**
- Document plan based on recovery strategies
- Incorporate recovery strategies into business practice

**Train, Exercise & Distribute Plan**
- Train team members on the plan
- Exercise the plan
- Distribute plan to all team members

**Maintain Plan & Improve BCM Capabilities**
- Maintain and re-distribute plans periodically or upon significant business change
- Conduct exercises of increasing complexity
- Periodically assess & improve recovery capabilities
Strategy selection – Business Continuity

Range of recovery alternatives for business function availability

People, Facilities, Logistics

- Prestaged workspace
- Commercial work area
- Dedicated workspace
- Remote access
- Mobile facility
- Acquisition

Cost of solution

Recovery Time Objective

- Seconds
- Minutes
- Hours
- Days
- Weeks
Strategy selection – Disaster Recovery

Range of recovery alternatives for IT application availability

Cost of solution

Networks, Computers, Applications

Automatic fail-over
Manual fail-over
Hot-site
Warm-site
Cold-site
Acquisition

Time to functional availability

Seconds → Minutes → Hours → Days → Weeks

$\$\$

34
Strategy selection – Data Backup & Recovery

Range of recovery alternatives for data protection

Data backup and recovery strategies

- Traditional data recovery
- Electronic vaulting
- Remote journaling
- Stand-by database
- Asynchronous replication
- Synchronous mirroring

Recovery Point Objective
- Days
- Hours
- Minutes
- Seconds
- Zero

Cost of solution

$$$

Zero
Session Agenda

1. Why Care?
2. Key Terminology
3. HIPAA Regulatory Requirement
4. How to Get Started
5. Specific, Practical Best Practices
6. Business Impact Analysis Exercise
Practical Five-Step Planning Process

1. Prioritize Business Processes
2. Determine Business Objectives
3. Identify Data Loss Scenarios
4. Bring it All Together
5. Communicate, Practice & Refine
1. Prioritize Business Processes

A. Review the business work flow / processes and how the business functions.
B. Ask: how long would your organization continue to operate without its key business processes?
C. Identify computing infrastructure, key applications or its data that support those processes?
D. Estimate the business value lost if data and/or applications and/or infrastructure are not available
E. Set a relative priority or “tiering” of processes and data, applications and infrastructure

Make this a business project! ... not an IT Project !!!

HBMA Healthcare BILLING & MANAGEMENT Association

38
2. Determine Business Objectives

A. Use the established relative priority of your business processes, data, business applications and infrastructure

B. Determine your Recovery Time Objectives (RTO) for each key business process, database, business application and infrastructure component

C. Determine your Recovery Point Objectives (RPO) for each key business process, database, business application and infrastructure component

D. Identify the types and scope of the Data Loss Events (DLE) against which you seek protection.

One size does not fit all! It’s about your Businesses Processes!
3. Identify Data Loss Scenarios

A. Use the list of potential Data Loss Events on which you will focus
B. Assess the probability (think frequency) of each event occurring
C. Assess the severity (think impact or loss) associated with each event occurring
D. Compute the potential business loss
E. Finalize the Data Loss Events on which your plan will focus
## Probability versus Severity Matrix for Data Loss Events

<table>
<thead>
<tr>
<th>Probability of Data Loss Event</th>
<th>Severity of Data Loss Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>H</td>
<td>3</td>
</tr>
<tr>
<td>M</td>
<td>2</td>
</tr>
<tr>
<td>L</td>
<td>1</td>
</tr>
<tr>
<td>L</td>
<td>L</td>
</tr>
</tbody>
</table>

*Use above matrix to assess and rank order the data loss events against which you need protection.*
4. Bring It All Together

A. Assemble the prioritized business processes and underlying databases, applications and infrastructure

B. Assemble your RTO and RPO goals for each prioritized business process

C. Confirm the identified data loss events and costs

D. Document the complete plan for each tier of business process (and underlying databases, applications and infrastructure relative to the scope of the data loss event)
## Useful Conceptual Framework

<table>
<thead>
<tr>
<th>TIER</th>
<th>RTO</th>
<th>RPO</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Tier 1 - Mission Critical</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EMR System</td>
<td>2 hrs</td>
<td>15 min</td>
</tr>
<tr>
<td>Filmless Radiology</td>
<td>8 hrs</td>
<td>15 min</td>
</tr>
<tr>
<td>Practice Management System</td>
<td>8 hrs</td>
<td>60 min</td>
</tr>
<tr>
<td><strong>Tier 2 - Business Critical</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MS Exchange E-mail System</td>
<td>24 hrs</td>
<td>15 min</td>
</tr>
<tr>
<td>Great Plains Accounting System</td>
<td>16 hrs</td>
<td>30 min</td>
</tr>
<tr>
<td><strong>Tier 3 - Departmental Important</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Web Site</td>
<td>48 hrs</td>
<td>24 hrs</td>
</tr>
</tbody>
</table>

### Considerations
- Correlate to risk and potential loss
- Business value versus Budget
5. Communicate, Practice & Refine

A. Assemble key staff involved in recovery operations
B. Designate key leadership roles
C. Identify modes of emergency communications
D. Create “communications tree”
E. Complete “desk checks” and plan “walk throughs”
F. Create “use cases” or test scenarios for DLEs
G. Conduct announced tests and simulations
H. Conduct unannounced tests
I. Refine the plan after testing at least annually
Business Resumption Planning Resources

- NIST SP800-34 Contingency Planning Guide for Federal Information Systems
- FEMA Emergency Planning Guide
- An Overview of the Disaster Recovery Planning Process
- Sample Business Recovery Plan
Session Agenda

1. Why Care?
2. Key Terminology
3. HIPAA Regulatory Requirement
4. How to Get Started
5. Specific, Practical Best Practices
6. Business Impact Analysis Exercise
Typical BIA Steps

1. Select individuals to interview for data gathering.
2. Create data gathering techniques (surveys, questionnaires, qualitative and quantitative approaches).
3. Identify the company’s critical business functions.
4. Identify the resources these functions depend upon.
5. Calculate how long these functions can survive without these resources.
6. Identify vulnerabilities and threats to these functions.
7. Calculate the risk for each different business function.
8. Document findings and report them to management.
Our Exercise

1. List your company’s critical business functions or processes

2. Choose **one process** (most critical) and then list all the resources this process depends upon.

3. Estimate your Recovery Time Objective for your chosen business process can survive without these resources.

4. Estimate your Recovery Point Objective for your chosen business process

5. Define your biggest potential threat sources (Adversarial, Accidental, Structural, Environmental)
Summary

- Get serious about business resumption planning
- Make it a business project, not an IT project
- Make it about your business
- Remember the key pieces
  - Business Continuity
  - Disaster Recovery
  - Data Backup and Restoration
- Remember: without your data, all else is for naught!
10-Point Data Protection Checklist

1. Backup Data; be 100% confident you can restore it!
2. Secure Network
3. Block Spam
4. Stop Malware
5. Condition Power
6. Patch Software
7. Encrypt Data
8. Practice Recovery
9. Enforce Policies
10. Insure Technology
Questions?

How Much Is It Worth?
Supplemental materials
Basic Risk Questionnaire

1. How does our organization identify critical or sensitive information assets and risks to those assets?
2. What is the value of our digital assets?
3. Is the frequency and scope of our risk evaluation and compliance audits sufficient to take evolving threats into account?
4. Are risks to critical or sensitive information assets managed in a similar fashion to other key business risks?
5. What is the structure, activities, and decision-making relating to cyber risk management, including electronic fraud?
6. What are our due diligence and financial responsibility (insurance) requirements for other companies that connect to our network or provide technology services?
7. How much have we invested in our IT infrastructure and does our risk transfer program reflect that investment?
8. How much risk can we afford to retain?
Technical recovery strategies

Once the business impact analysis and IT risk assessments are conducted, the results will decide how far a business would like to take its IT disaster recovery plan.

- **Level 0**: Improve current environment
- **Level 1**: Data duplication
- **Level 2**: Centralized storage and backup restore
- **Level 3**: Remote data duplication
- **Level 4**: Active secondary site
- **Level 5**: Advanced recovery

**Meeting recovery time objectives**
## Strategy selection

Summary description of business function availability alternatives

<table>
<thead>
<tr>
<th>Description</th>
<th>Relative cost</th>
<th>Recovery time</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Pre-staged workspace</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dedicated facility and infrastructure providing an</td>
<td>Floor space:</td>
<td>Zero to 8 Hours</td>
</tr>
<tr>
<td>immediate access to a replicated work environment</td>
<td>Infrastructure:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Network:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Total cost:</td>
<td></td>
</tr>
<tr>
<td><strong>Commercial work-area</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Shared vendor facility permitting rapid access to</td>
<td>Floor space:</td>
<td></td>
</tr>
<tr>
<td>workspace. PC’s, special equipment, and voice</td>
<td>Infrastructure:</td>
<td></td>
</tr>
<tr>
<td>applications are prepositioned</td>
<td>Network:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Total cost:</td>
<td></td>
</tr>
<tr>
<td><strong>Dedicated workspace</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dedicated facility requiring quick-shipment of</td>
<td>Floor space:</td>
<td></td>
</tr>
<tr>
<td>desktop PC’s, office equipment, and other</td>
<td>Infrastructure:</td>
<td></td>
</tr>
<tr>
<td>infrastructure</td>
<td>Network:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Total cost:</td>
<td></td>
</tr>
<tr>
<td><strong>Remote access</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Third-party offices and workstations connecting to</td>
<td>Floor space:</td>
<td></td>
</tr>
<tr>
<td>critical IT systems via remote access</td>
<td>Infrastructure:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Network:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Total cost:</td>
<td></td>
</tr>
<tr>
<td><strong>Mobile facility</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vendor shipped mobile facility to a pre-determined</td>
<td>Floor space:</td>
<td></td>
</tr>
<tr>
<td>location and configured for a rapid setup</td>
<td>Infrastructure:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Network:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Total cost:</td>
<td></td>
</tr>
<tr>
<td><strong>Acquisition</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Equates to time of disaster definition of recovery</td>
<td>Floor space:</td>
<td></td>
</tr>
<tr>
<td>strategy for alternate facilities, data network,</td>
<td>Infrastructure:</td>
<td></td>
</tr>
<tr>
<td>server/storage infrastructure, etc.</td>
<td>Network:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Total cost:</td>
<td></td>
</tr>
</tbody>
</table>

**Floor space:** $$$

**Infrastructure:** $$$

**Network:** $$$

**Total cost:** $$$
# Strategy selection

## Summary description of availability alternatives

<table>
<thead>
<tr>
<th>Description</th>
<th>Relative cost</th>
<th>Recovery time</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Automatic fail-over</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remote server clustering with application load balancing and/or intelligent fail-over processing</td>
<td>$$$$$</td>
<td>Zero to 60 Minutes</td>
</tr>
<tr>
<td><strong>Manual fail-over</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remote server clustering with manual fail-over requiring operator intervention</td>
<td>$$$$</td>
<td>60 Minutes to 12 Hours</td>
</tr>
<tr>
<td><strong>Hot-site</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Restoration of application processing to prestaged network and dedicated IS infrastructure</td>
<td>$$</td>
<td>12 Hours to 72 Hours</td>
</tr>
<tr>
<td><strong>Warm-site</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Restoration of application processing to prestaged network and limited IS infrastructure</td>
<td>$$</td>
<td>48 Hours to 5 Days</td>
</tr>
<tr>
<td><strong>Cold-site</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Restoration of IS to prestaged facility and utility. Infrastructure acquired at time of disaster</td>
<td>N/A</td>
<td>96 Hours to 14 Days</td>
</tr>
<tr>
<td><strong>Acquisition</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Best effort at time of disaster to acquire facility and infrastructure. Data restored from tape backup</td>
<td>N/A</td>
<td>10 Days to 30 Days</td>
</tr>
</tbody>
</table>

### Cost Breakdown

- **Storage**: $$$$$
- **Hosts**: $$$$$
- **Network**: $$$$$
- **Facilities**: $$$$$
# Strategy selection

## Summary description of data recovery alternatives

<table>
<thead>
<tr>
<th>Description</th>
<th>Relative cost</th>
<th>Data recovery point</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Synchronous mirroring</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Real-time remote Disk volume mirroring (Equivalent to remote RAID-1)</td>
<td>Storage: $$$$ Hosts: $$ Network: $$$ Tape: N/A</td>
<td>Zero data loss</td>
</tr>
<tr>
<td><strong>Asynchronous replication</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Near real-time remote disk volume mirroring or data replication</td>
<td>Storage: $$$ Hosts: $$$ Network: $$ Tape: $$$</td>
<td>Data recovery within seconds to minutes of last transaction, track change, or other delta</td>
</tr>
<tr>
<td><strong>Stand-by database</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remote transaction Journaling or vaulting as Applied to a standing database</td>
<td>Storage: $$ Hosts: $$ Network: $$ Tape: $$$</td>
<td>Data recovery within seconds or minutes of point of failure</td>
</tr>
<tr>
<td><strong>Remote journaling</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remote transaction data recovery near to point of failure</td>
<td>Storage: $$ Hosts: $$ Network: $$$ Tape: $$</td>
<td>Data recovery within seconds or minutes of point of failure</td>
</tr>
<tr>
<td><strong>Electronic vaulting</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bulk data transfer to remote tape/disk as triggered by time or event</td>
<td>Storage: $$ Hosts: $$ Network: $$ Tape: $$</td>
<td>Data recovery within minutes or hours of point of failure</td>
</tr>
<tr>
<td><strong>Traditional data recovery</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Weekly, nightly or intraday backup to off-line tape media that is manually moved off-site</td>
<td>Storage: $$ Hosts: $$ Network: $$ Tape: $$</td>
<td>Data recovery within hours or days of point of failure</td>
</tr>
</tbody>
</table>
What Cost, Business Interruption?

- $BI = T \times Q \times V$, where:
  - $BI$ = business interruption
  - and:
    - $T$ = the number of time units (hours, days) operations are shut down
    - $Q$ = the quantity of goods or services normally produced, or sold, per unit of time used in $T$
    - $V$ = the value of each unit of production, usually expressed in profit

- Plus, potentially…
  - Negative publicity
  - Loss of clients
  - Legal liability
What Cost, Business Interruption?

Example 1…
- Attorney, bills @ $175.00 per hour
- Server crashes and requires one week to restore
- \[ BI = \text{business interruption cost} = BI = T \times Q \times V \]
- \[ = 40 \times 1 \times \$175 \]
- \[ = \$7,000.00 \text{in missed revenue} \]

Example 2…
- Medical office, admin staff of 5 earning $15.00 per hour
- Server crashes and requires 3 days to restore
- \[ BI = \text{business interruption cost} = BI = T \times Q \times V \]
- \[ = 24 \times 5 \times \$15.00 \]
- \[ = \$1,800.00 \text{in lost productivity} \]
“7- Deadly Sins” Exercise

1. Did you back up your data in the last 24 hours?
2. Did you review the logs to see if it worked?
3. Did you take your backup disk or tape offsite in the last 24 hours?
4. Have you tested your restore capability in the last 30 days?
5. Do you have written data backup policies & procedures that you follow?
6. Do encrypt tape and/or disk media backup?
7. Are you fully compliant with HIPAA Security (Contingency Plan Standard)?
All Types of Data Loss Events:
File corruption, server failure, and site failure
Recovery times and points remain a key consideration for most companies.
## Typical Roadmap for BC/DR Project

<table>
<thead>
<tr>
<th>MAJOR PROJECT PHASE</th>
<th>Month 1 (3 day effort)</th>
<th>Month 2 (8 day effort)</th>
<th>Month 3 (8 day effort)</th>
<th>Month 4 (Effort TBD)</th>
</tr>
</thead>
<tbody>
<tr>
<td>BC/DR Program Standards</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data Gathering Workshops</td>
<td></td>
<td>(8 day effort)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Develop Recovery Strategy</td>
<td></td>
<td>(8 day effort)</td>
<td>(Effort TBD)</td>
<td></td>
</tr>
<tr>
<td>Plan Development</td>
<td></td>
<td>(5 day effort)</td>
<td>(5 day effort)</td>
<td></td>
</tr>
<tr>
<td>Education and Awareness</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Plan Refinement</td>
<td></td>
<td></td>
<td>(5 day effort)</td>
<td></td>
</tr>
<tr>
<td>Develop Program Structure</td>
<td></td>
<td></td>
<td>(6 day effort)</td>
<td></td>
</tr>
</tbody>
</table>