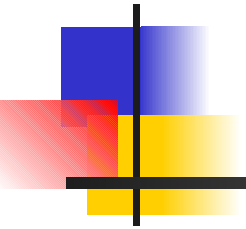


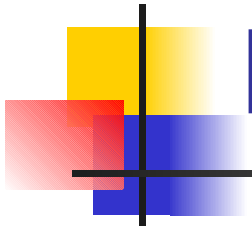
Disaster Recovery & Business Continuity

Ing. Stefano Zanero, Secure Network

Ing. Yvette Agostini, Sikurezza.org

Di cosa ci occupiamo

- Contingency Planning
  - Disaster Recovery
  - Business Continuity
  - Incident Response
- Tutto questo richiede
  - Riorganizzazioni dei processi aziendali
  - Analisi dei rischi
  - Intervento sulle infrastrutture IT



Disastri

Disastri naturali: terremoto, alluvione, tornado, eruzioni, ma anche semplicemente una tempesta...
Disastri dovuti all'uomo e alla tecnologia: incendio, esplosione, mancanza di corrente, di linee telefoniche e dati o di condizionamento ambientale
Disastri fortuiti
- Le coincidenze congiurano sempre per produrre il massimo danno possibile (legge di Murphy)

Non è solo questione di sicurezza informatica...
- Priorità all'incolumità delle *persone*: si tratta di un requisito etico fondamentale

... Ma non succede mai ...

Solo per i tornado: 102 emergenze negli USA negli ultimi 10 anni

Alluvioni: altro grande problema spesso sottovalutato, specie in Italia...

Una compagnia USA su 4 ha dichiarato di avere attraversato un disastro negli ultimi 5 anni

“Non ci è mai successo...”

- Di avere un virus informatico sulla rete ?
- Che l'ENEL ci lasciasse al buio ?
- Che le linee dati saltassero ?
- ... datemi il vostro indirizzo !

Ma quanto danno può fare ?

Terremoto in California del 94: piu' di 6 miliardi di EUR !

Anche l'italia è sismica...

Negli anni '90 negli USA la FEMA ha speso piu di 20 miliardi di EUR per interventi nei disastri

Quanto siamo preparati ?

Solo il 68% delle compagnie hanno un BCP, e solo il 55% di queste lo hanno provato...

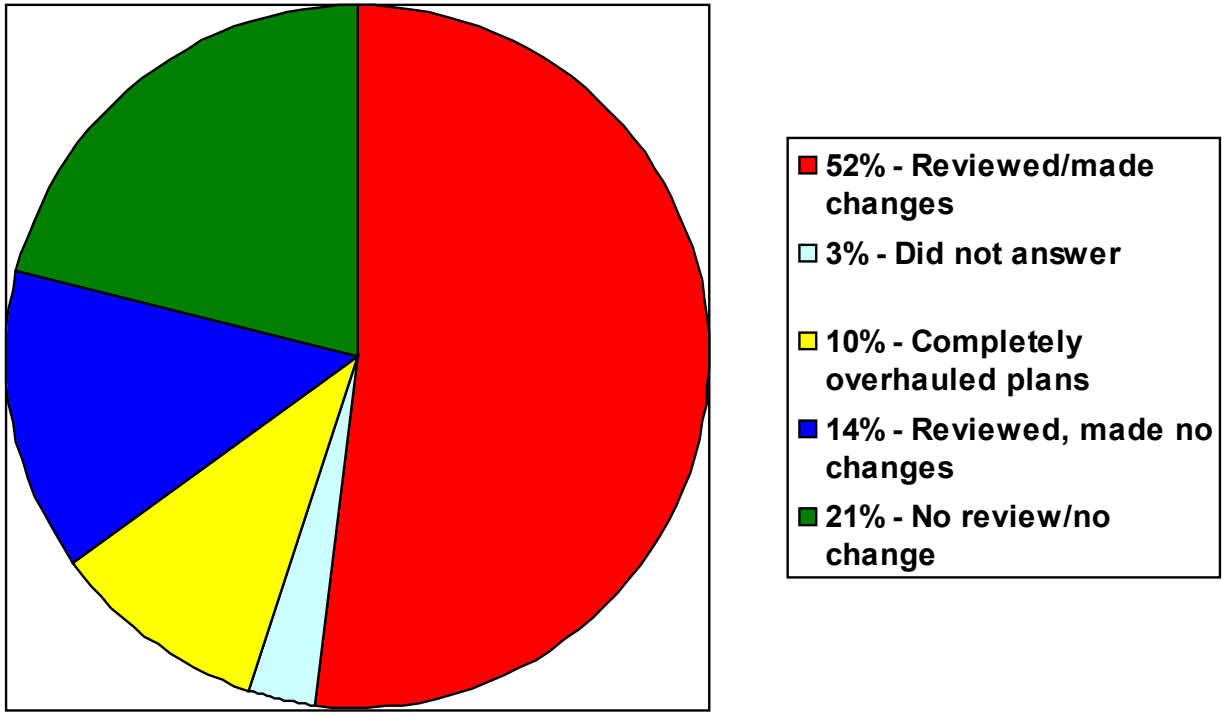
L'87% esegue backup giornalieri

Il 20% delle compagnie ha un RTO di meno di 24 ore, ma solo il 44% lo ha verificato!

Il 64% delle imprese non sono preparate a disastri che coinvolgano la loro connessione WAN, e il 25% nemmeno LAN

Chi ha fatto i compiti ?

Chi ha aggiornato i CP dopo l'11 settembre 2001 ?



Contingency Planning & Management magazine and Strohl Systems Survey,
Jan 15-31. Total respondents: 1,437

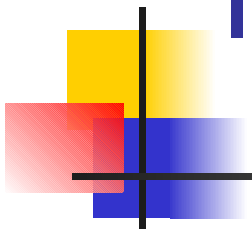
E se non siamo preparati ?

Fatte 5 le aziende colpite da un disastro esteso:

- Due non riaprono proprio
- Una riapre e fallirà entro due anni

80% delle aziende colpite dall'uragano Andrew e prive di un BCP sono fallite entro due anni dall'evento...

Il chiodo e il regno



Per colpa di un chiodo si perse uno zoccolo... per colpa della guerra il regno

Tanti piccoli disastri possono essere molto peggio per la baseline di un grosso disastro

A volte il BCP e il DRP contemplano solo i macrodisastri

Altre motivazioni

Problematiche assicurative

Problematiche di Auditing fiscale

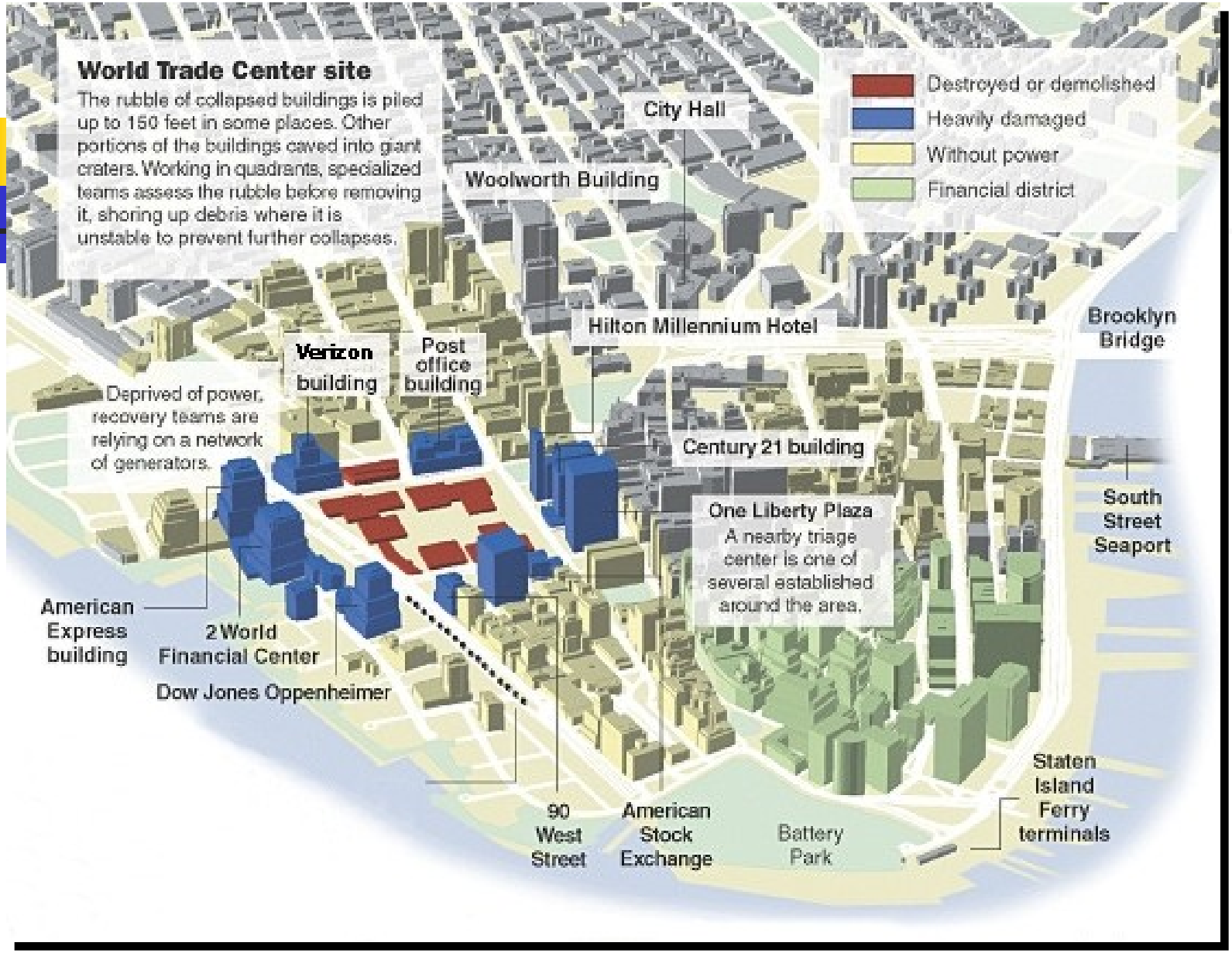
Requisiti di legge (Dlgs 196 ad esempio)

“Due diligence”

Basilea-2

Obblighi verso gli stakeholders

Sarbanes – Oaxley (SOX)


World Trade Center site
The rubble of collapsed buildings is piled up to 150 feet in some places. Other portions of the buildings caved into giant craters. Working in quadrants, specialized teams assess the rubble before removing it, shoring up debris where it is unstable to prevent further collapses.
Destroyed or demolished
Heavily damaged
Without power
Financial district
City Hall
Woolworth Building
Hilton Millennium Hotel
Brooklyn Bridge
Verizon building
Post office building
Deprived of power, recovery teams are relying on a network of generators.
Century 21 building
One Liberty Plaza
A nearby triage center is one of several established around the area.
South Street Seaport
American Express building
2 World Financial Center
Dow Jones Oppenheimer
90 West Street
American Stock Exchange
Battery Park
Staten Island Ferry terminals

Cos'è il Contingency Plan ?

Pianificazione per gli eventi inattesi

- L'uso della tecnologia potrebbe essere impossibile
- Il business aziendale è in sofferenza
- L'azienda rischia gravi danni

Significa preparare procedure che assorbano l'impatto dell'evento inatteso sul nostro business

Perchè serve un piano ?

- Perchè altrimenti durante l'emergenza potremmo essere incapaci di reperire risorse
- Perchè “durante” non siamo lucidi quanto “prima”
- Perchè le persone sbagliano sotto stress

Obiettivi del contingency plan

Ripristino del normale andamento operativo dell'azienda

- In termini di processi
- In termini di strutture
- In termini economici

Minimizzazione dei costi in tutti i sensi

Minimizzazione dell'impatto sul business

I componenti di un CP

Incident response plan (IRP): per fornire un'immediata risposta a situazioni critiche

Business continuity plan (BCP): l'insieme delle misure progettate per continuare ad operare in emergenza

Disaster recovery plan (DRP): focalizzato sul ripristino delle condizioni operative normali

(non sono nomenclature standard)

Un esempio di Timeline

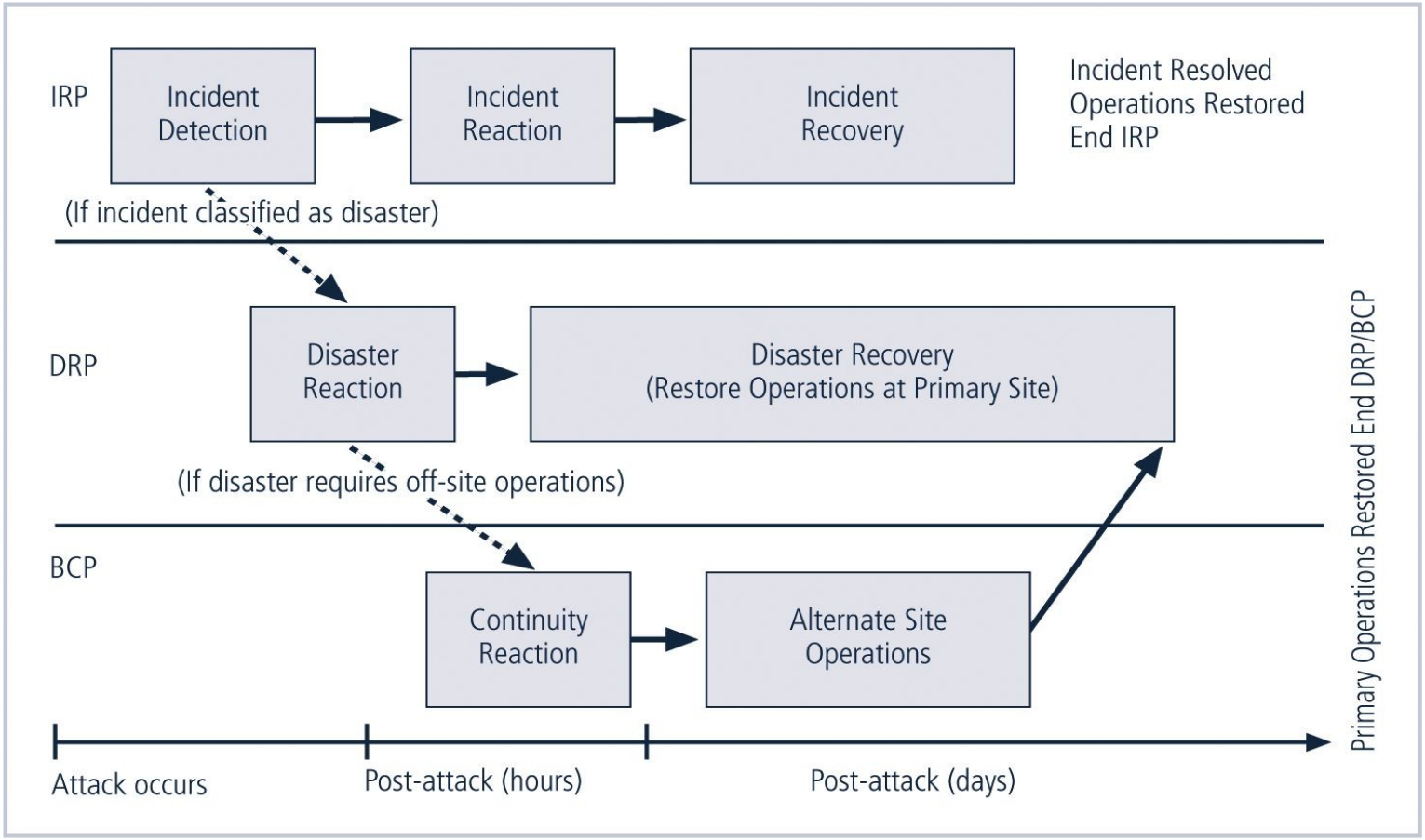


FIGURE 3-5 Contingency Plan Implementation Timeline

DRP vs BCP

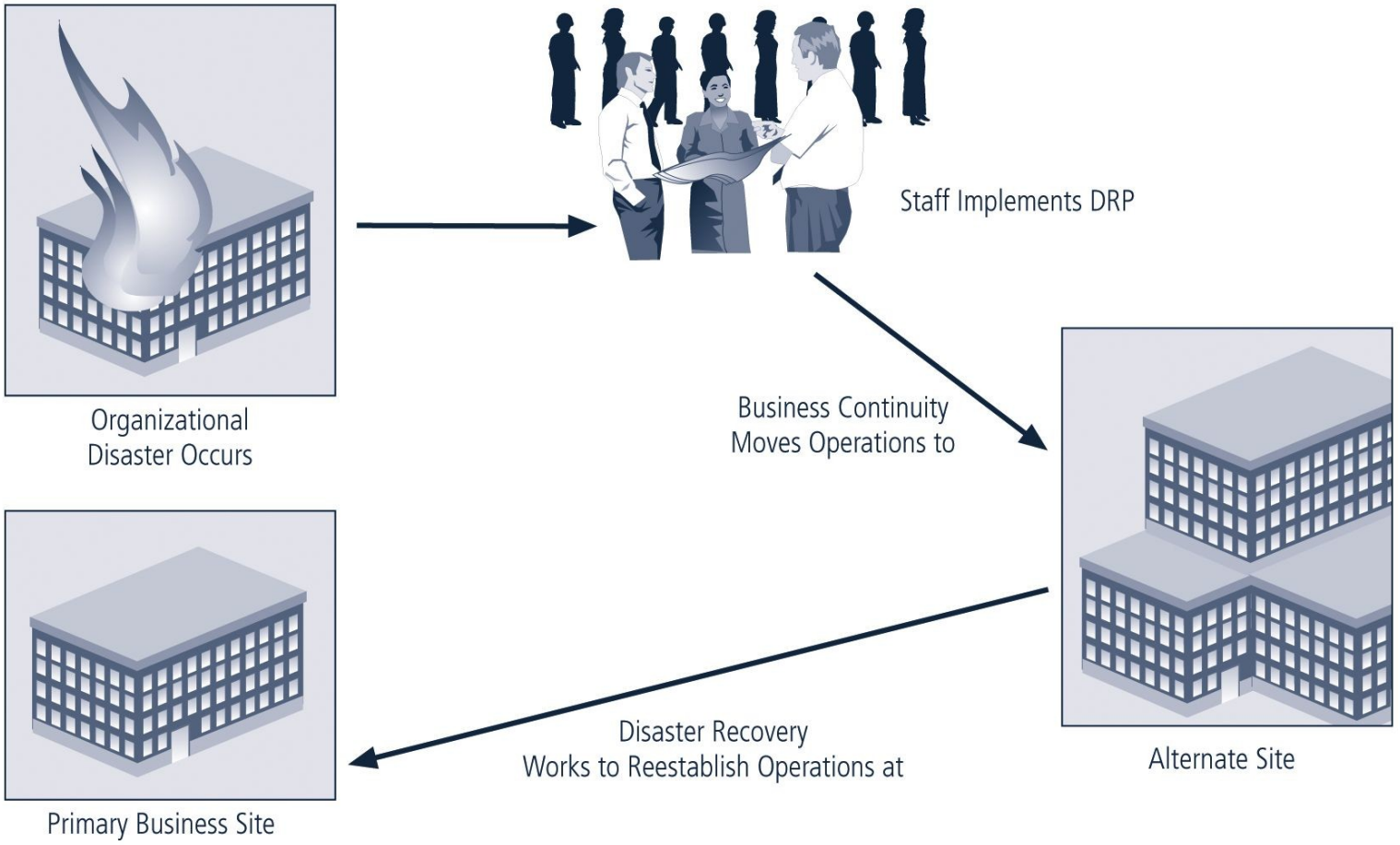
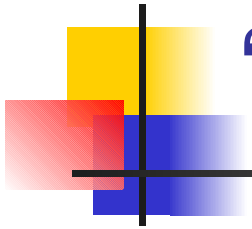


FIGURE 3-4 Disaster Recovery and Business Continuity Planning

Il percorso per creare un CP

- Risk Assessment e Business Impact Analysis
- Pianificazione strategica
- Implementazione e predisposizione dei piani
- Testing ed aggiornamento



“If you didn't test it...”

... it **doesn't work**

Cinque modi per testare un CP:

- Desk Check (il meno affidabile)
- Walkthrough/Roleplay
- Simulazione
- Testing in parallelo alle attività (a volte impossibile)
- Interruzione sperimentale e failover (rigoroso, rischioso)

Meglio scoprire i problemi quando l'emergenza è finta, che quando è vera...

NON PROVATELO UNA VOLTA SOLA !

I test possono anche essere “non annunciati”...

Risk Assessment

Necessaria per una valutazione costi/benefici (le misure di BCP riducono il rischio operativo, non hanno ROI diretto)

Identificazione degli **asset**

- Le persone (!)
- I processi di business principali
- Gli asset fisici e le risorse che supportano le funzioni critiche

Identificazione delle **minacce**

Identificazione delle possibili **vulnerabilità**

Vulnerabilità x Minaccia x Valore Asset = Rischio

Business Impact Analysis

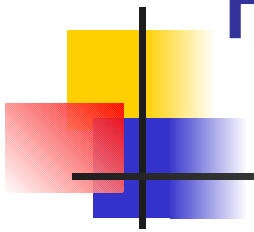
Cosa fa ?

- Prende le informazioni sui sistemi/processi di business e le minacce/vulnerabilità e le elabora in dettagliati scenari d'attacco
- Risk management usa le informazioni per elaborare contromisure
- BIA invece studia gli effetti del disastro nel caso colpisca e oltrepassi le contromisure

Le 4 fasi di una buona BIA:

- Identificazione delle minacce (come per risk analysis)
- Analisi e prioritizzazione delle business unit
- Scenari di disastro
- Assessment del danno potenziale

Pianificazione



Esiste un ordine logico con cui preparare un CP

- Prima, bisogna pensare a cosa fare **durante** l'incidente (quindi, l'IRP e il BCP)
- Poi bisogna pensare a cosa fare **dopo** l'incidente per ripristinare (quindi, il BCP e il DRP)
- Infine bisogna pensare a tutte le preparazioni da fare in anticipo per tutte le componenti del piano

Pianificazione=coinvolgimento

Piazzare 350 pagine di CP sulla scrivania significa invitare a non leggere

Business continuity: devo interrogare e interagire con chi si occupa del business

Le altre parti possono essere più “riservate agli addetti ai lavori”

Per il risk assessment è *fondamentale* il coinvolgimento del ramo direttivo e operativo dell'azienda !

Schematizzando...

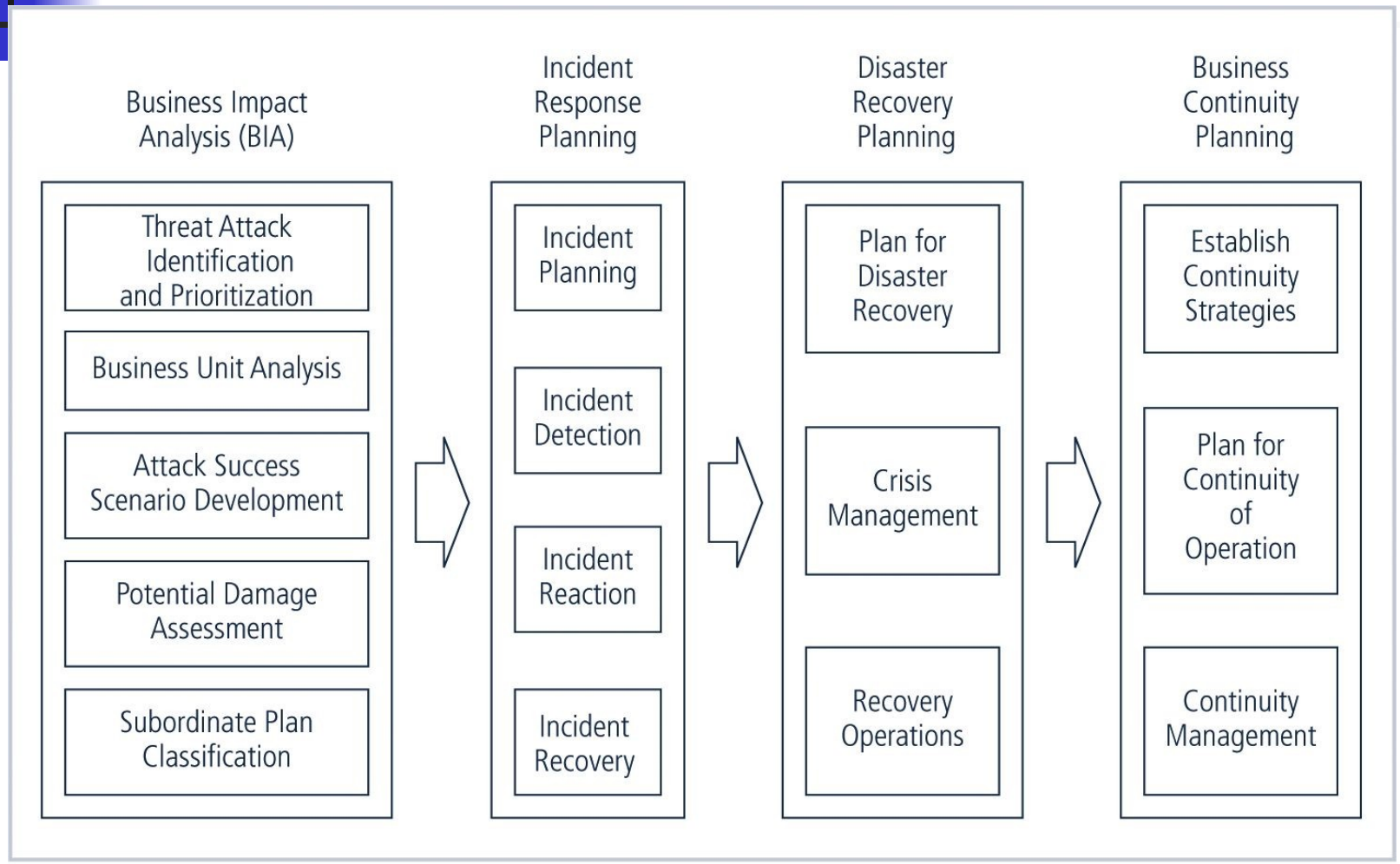
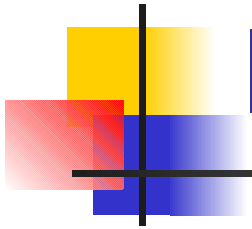


FIGURE 3-6 Major Tasks in Contingency Planning



Incident Response

- Elemento chiave dell'IR: il personale
  - Pronto, preparato e conscio del suo ruolo
  - Motivato e formato
  - Capace di agire in team
- Le fasi dell'Incident Response
  - Detection
  - Notification
  - Resolution/Escalation
  - A margine: Documentation

Incident Containment

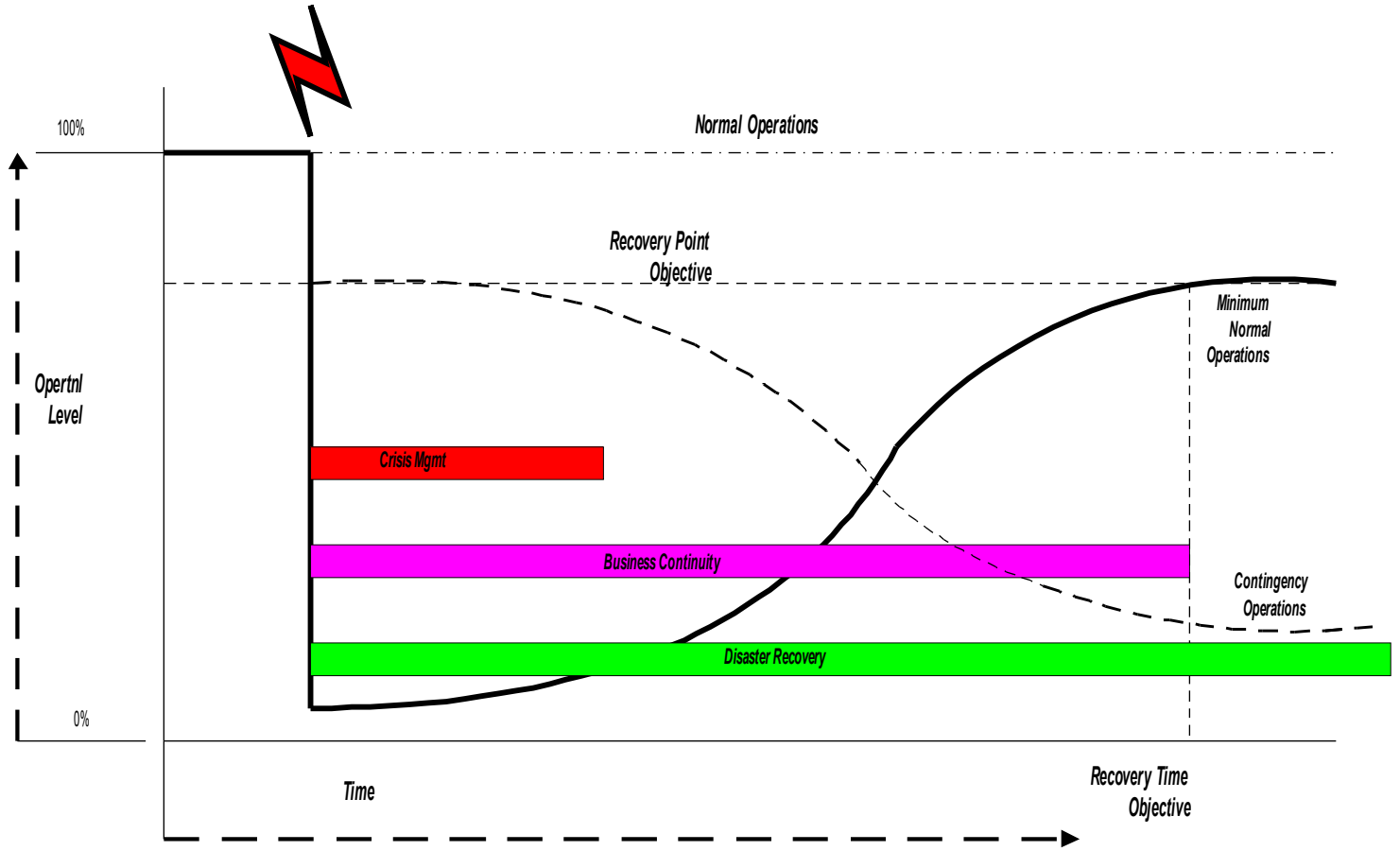
Il compito fondamentale di una azione di IR è di bloccare l'incidente, contenere il suo impatto, eventualmente scalare

Due task chiave:

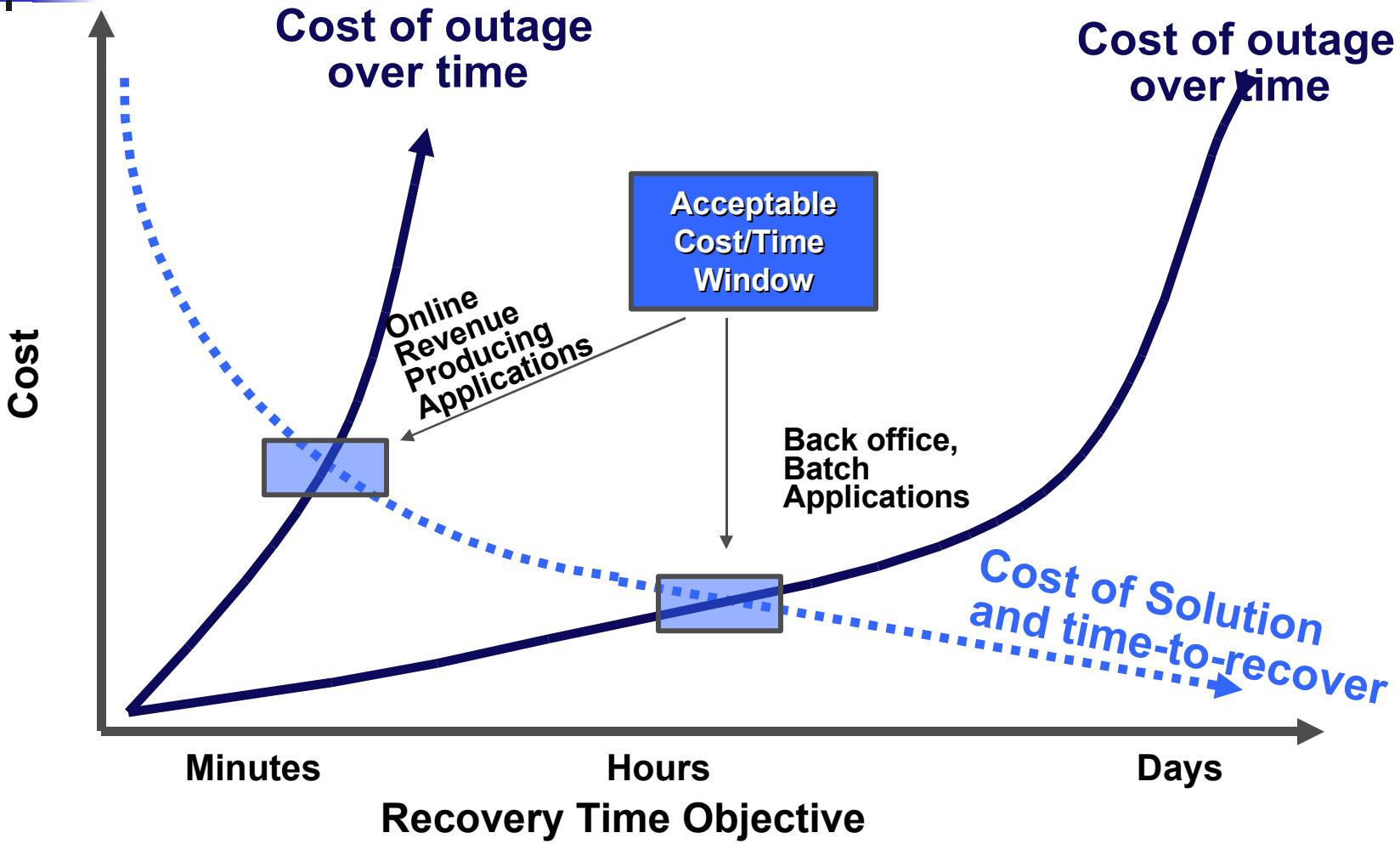
- Bloccare in tutti i modi l'incidente
- Recuperare la disponibilità dei sistemi in ordine di priorità

Ultimo task, se necessario: attivare la escalation

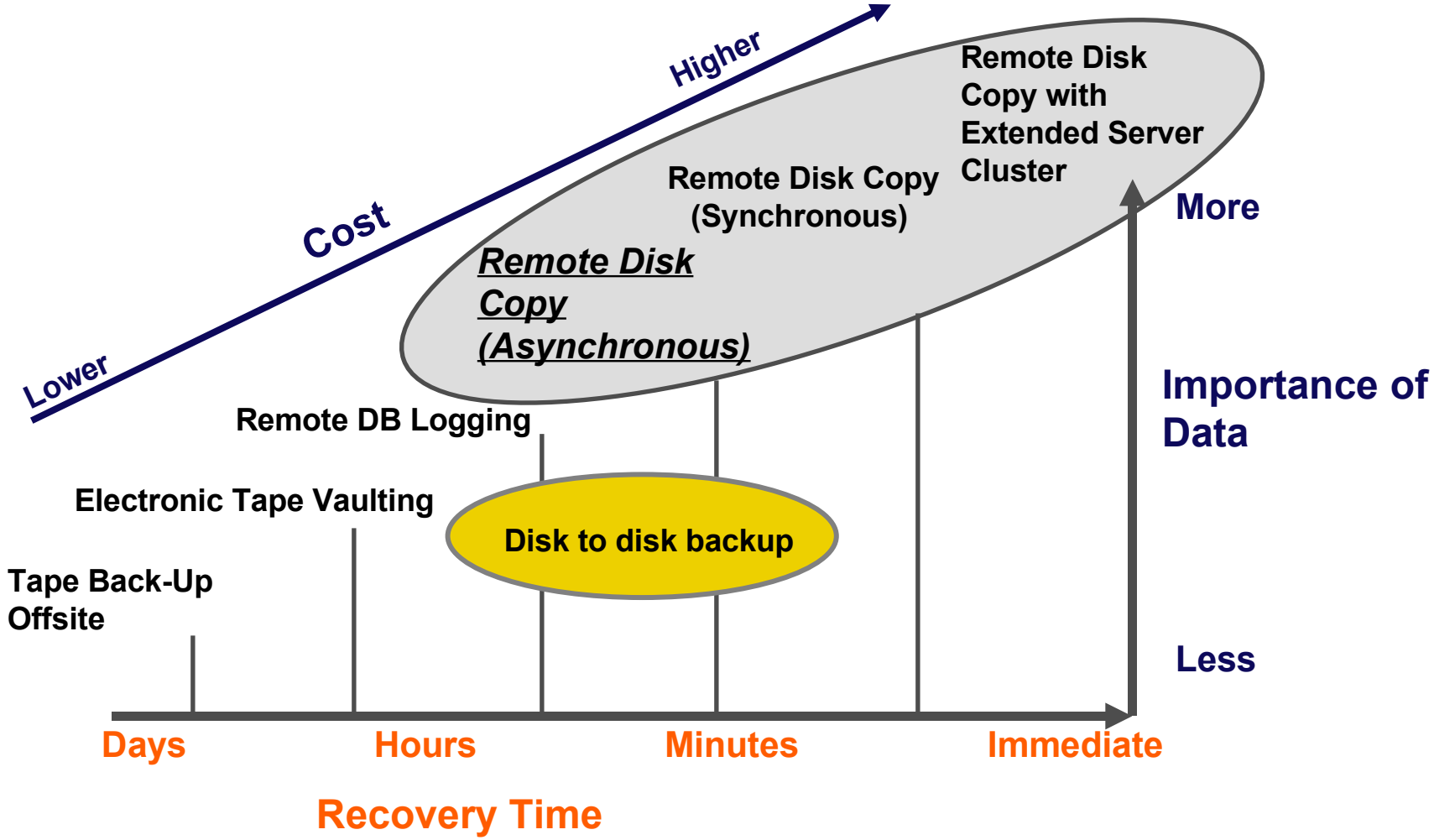
RTO vs RPO


100%
Normal Operations
Recovery Point Objective
Minimum Normal Operations
Opertnl Level
Crisis Mgmt
Business Continuity
Contingency Operations
Disaster Recovery
0%
Time
Recovery Time Objective

Non esiste un solo RTO



Esempio di valutazione RTO



Recovery: i passaggi chiave

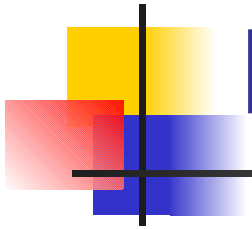
Identificare e risolvere la vulnerabilità che ha causato il disastro

Ripristinare dati, sistemi e servizi (dai backup)

Ripristinare e verificare i processi compromessi dal disastro

Installare, aggiornare o potenziare i meccanismi di contenimento che non hanno funzionato o che mancavano

Aggiornare le capacità di monitoraggio perchè aiutino nell'identificazione, e usarle per un continuo controllo dei sistemi



Business Continuity Plan

- Lo scopo è garantire la continuità del business
- La leadership qui è di business, non tecnica!
- Si esegue in parallelo al DRP e all'IR, se necessario
- Spesso costoso, quindi “last resort”
- Meccanismo: spostamento delle funzioni critiche di business su un sito alternativo
- Dobbiamo quindi identificare le funzioni critiche, ed equipaggiare il sito alternativo

Opzioni ad uso esclusivo

Hot Site

Centro completo di computer, preconfigurato, con tutti i servizi pronti al subentro, incluse facilities aggiuntive e luoghi per il personale

Warm Site

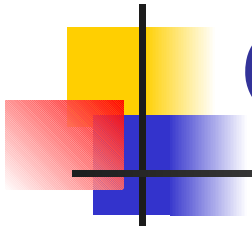
Come l'hot site, ma non completamente pronto al subentro, e magari con facilities da attivare

Cold Site

Servizi informatici ridotti e non preparati (solo infrastruttura). Servizi di emergenza.

Opzioni in condivisione

- Timeshares
  - “Affittiamo” un'opzione su un sito di recovery
  - Potremmo non avere la priorità quando serve !
- Accordi interaziendali
  - Io aiuto te e tu aiuti me in caso di bisogno
  - Devo pianificare potenza e spazi in esubero
- Alcune alternative esotiche
  - “Rolling mobile sites”
  - Contratti per forniture d'emergenza



Off-Site Data Storage

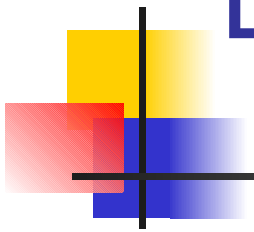
È fondamentale pensare a come trasferire i dati più aggiornati possibile al sito secondario

Tra le opzioni:

- Electronic vaulting: trasferimento batch dei backup verso uno storage off-site
- Remote Journaling: trasferimento live delle transazioni sotto forma di journal
- Database shadowing: uso ridondato dei database principale e secondario

Cambiano chiaramente costo, impatto prestazionale, RTO e RPO

Logistica



Il personale deve poter raggiungere il sito di backup

Che fare se l'aeroporto si allaga ?

Materiale importante da salvare e spedire

Cibo, acqua, eventuale alloggio per team di emergenza

Telecomunicazioni dal sito secondario

Infrastrutture critiche

Come tecnologi, il nostro focus primario sono le infrastrutture tecnologiche

In particolare dobbiamo considerare

- Telecomunicazioni (WAN, telefonia, etc)
- Infrastruttura di rete (LAN/MAN)
- Architetture di HA, hot/warm/cold site, etc.
- Sistemi di storage e replicazione per la **protezione dei dati (fondamentale)**

Quanto segue va considerato come un esempio, non come esaustivo

Telefonia e connettività

- Un sito primario o secondario senza telefonia e/o connessione dati è quasi inutile
  - All'attivazione del secondario dovrebbe seguire immediatamente il rerouting
- Valutazione delle vulnerabilità nella connettività:
  - Determinazione dei SPOF
  - Prioritizzazione delle connessioni
- È comunque necessario considerare
  - Linee entranti
  - Linee tra sito primario e secondario
  - Linee che generano revenue
  - Linee uscenti per il team di crisis management

... e se è l'ora del pilota ?

Vecchia battuta: “Perchè hai paura di volare? Tanto, se non è la tua ora...” “...e se fosse l'ora del pilota?”

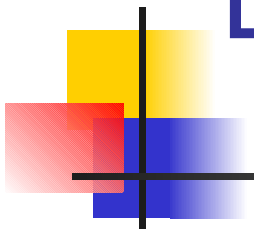
Che succede se il disastro colpisce il nostro provider ?!

È necessario prevedere connessioni ridondate di backup (anche sottodimensionate, eventualmente)

Se il disastro fosse geografico, potrebbe non bastare: di nuovo, il sito secondario è necessario

- Sarebbe anche possibile usare coperture satellitari

Esempio di SPOF: il call center



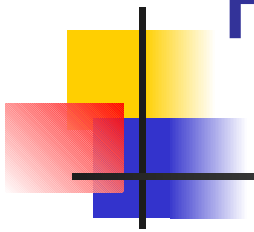
I call centers sono molto vulnerabili

- Tipicamente revenue-generator
- Tipicamente accentrati in una singola struttura
- Tipicamente posizionati “fuori mano”

Per evitare l'effetto SPOF, consideriamo

- La creazione di un centro alternativo (costa)
- L'uso di call center condivisi (rischioso !)
- Dividere il call center per funzioni in due luoghi diversi, e cross-addestrare gli operatori

Perchè i dati sono critici



- Perchè sono l'unico asset completamente irrecuperabile
- Perchè sono l'asset più fragile
- Perchè sono, in generale, l'unica cosa di cui ci importi veramente
- Come salvare i dati ?
  - Non è sempre facile
  - Tre strategie fondamentali:
    - Registrazione su media di backup (nastro)
    - Duplicazione fuori linea
    - Duplicazione in line

Il nastro è morto. O no ?

- “Il nastro è morto: meglio le SAN”
  - **Molte delle SAN vengono usate per condividere i dispositivi a nastro**
- “Il nastro è troppo lento per i volumi di dati moderni” (?!?)
  - **Ma è proprio vero ? Vedremo le tecnologie nuove**
  - **Gran parte dei DB sono statici nella parte storica, e incrementalmente aggiornati: possiamo fare backup incrementale su nastro**
  - **Il mirroring non è esattamente privo di problemi...**

Pro e Con del Mirroring

PRO

- Velocità nel RTO
- RPO nullo
- Efficacia, affidabilità
- Flessibilità nel recovery
- Nuove tecnologie come ad esempio Wavelength Division Multiplexing stanno riducendo il costo della connessione WAN/MAN in fibra

CON

- Va comunque monitorato
- Spesso il software di mirroring è vendor-specific
- Spesso, per ridurre la latenza sulle applicazioni on line, serve una configurazione a tre livelli
- Soluzione ad altissimo costo
- Mirroring con consolidamento o virtualizzazione: problemi di performance in scrittura

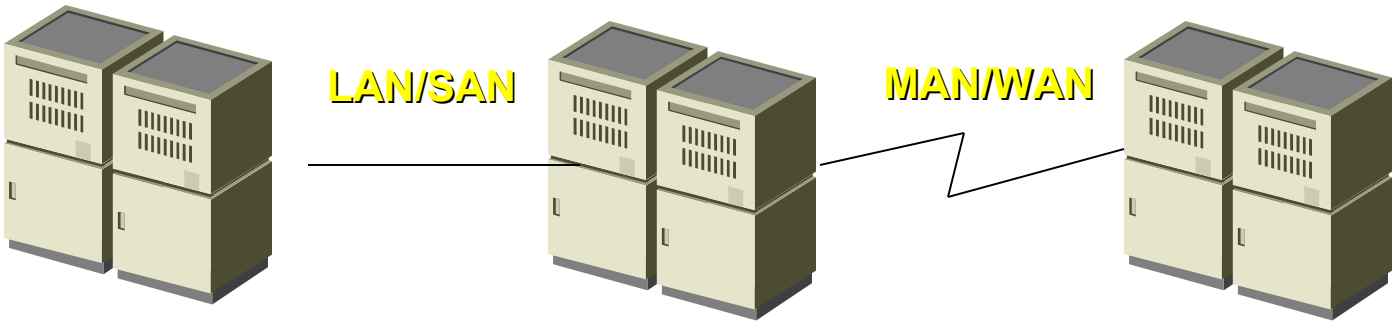
Pro e Con del nastro

PRO

- Costo inferiore
- RTO ed RPO dipendono dalla strategia ma si possono ottimizzare
- La gestione dei nastri robotizzata risolve molti problemi
- Volumi e throughput dei dati sono ormai gestibili
- Il nastro in un caveau è una soluzione di ultima spiaggia per i disastri peggiori

- CON
  - I nastri sono mezzi fisici fragili, è necessario il vaulting
  - Problemi di performance in ambienti virtualizzati
  - La differenza di prezzi coi dischi si è parzialmente ridotta
  - Avere i dati online è comunque meglio che avere i dati quasi online

L'ottimo sarebbe...



MIRROR SIMMETRICO (LOCALE, BASSA LATENZA)

MIRROR ASIMMETRICO (REMOTO, NON SINCRONO)

Problema di disastro geografico

Problema di ripartenza

Risorse web

http://www.thebci.org/
http://www.nysfirm.org/healthcheck.asp
http://www.bcpa.org/
http://www.utoronto.ca/security/drp.htm
http://www.disasterrecoveryworld.com/
http://www.disasterplan.com/
www.npa.org
www.globalcontinuity.com
www.drii.org
www.acp-international.com
www.contingencyplanningresearch.com
www.drj.com
www.disaster-help.com
www.e-janco.com/drp.htm

Risorse web

http://www.drie.org
http://www.globalcontinuity.com
http://www. upenn.edu/audit/what/best_practices.htm
http://www.survive.com
http://www.idra.com
http://www.disaster.net
http://www.vita.org
http://www.issa.org/disaster.htm
http://www.dir.state.tx.us/security/continuity/index.html

Contatti

Yvette Agostini

yvette@yvetteagostini.it

Stefano Zanero

s.zanero@securenetwork.it