Disaster

-คือ เหตุการณ์ณ์ที่ไปขัดขวางหรือไปหยุดการทำงาน

DR plan ที่ดีต้องลดการตัดสินใจ สามารถหยิบมาใช้ได้เลยเพราะ เหตุการณ์ณ์มันฉุกเฉินมาก

Natural Disasters

-Earthquakes

-Flood รวมไปถึงสึนามิ, flash flood คือน้ำท่วมแบบฉับพลัน

-Storms (hurricane,tornado,lighting:ฟ้าผ่า)

-fire:ไฟไหม้ รวมไปถึง ไฟป่า:wildfire

-Volcanic eruption:ภูเขาไฟระเิด, mudslide:ดินสไลด์, avalanche:หิมะถล่ม, monsoon:มรสุม

Man-made Disasters

-Fires

-Acts of Terrorism

-Bombings/Explosions

-Power Outages

-Other Utility and Infrastructure Failures : เช่นระบบน้ำ ท่อน้ำ ท่อแตกสามารถรั่วมาใส่อุปกรณ์อิเล็กทรอนิกได้

-Hardware/Software Failures : ความขัดคล่องของ hw sw การจะรับมือต้องมีระบบ redundant การทำสำรอง แต่ค่าใช้จ่ายสูงมาก บางองค์กรก์ทำไม่ได้

-Strikes/Picketing : การหยุดงานหรือการประท้วง

-Theft/Vandalism : การทำร้ายข้อมูล หรือการบ่อนทำลาย

Understand System Resilience and Fault Tolerance

- เป้าหมายคือป้องกัน single point of failure เช่น ถ้า ดิสท์มันพังมันก็จะทำให้ทั้ง server พังได้

- Fault Tolerance : ความสามารถในการทดความผิดพลาดและยังทำงานต่อไปได้ เช่น redundant ทำ RAID, failover cluster

- System Resilience(ความสามารถในการกู้คืน) คล้าย Fault Tolerance ที่ยังสามารถทำงานต่อเนื่องได้ แต่ต้องอยู่ในระดับที่ยอมรับได้ด้วย

Protecting Hard Drives, RAID configurations

RAID-0 : ใช้เทคนิค striping เก็บข้อมูลไขว้กันไป ข้อดีคือ ประสิทธิภาพที่ดี แต่ไม่ทดทานต่อความผิดพลาด

RAID-1 : เก็บข้อมูลเหมือนๆ กัน

RAID-5 : striping + priority, ต้องมีดิสด์อย่างน้อยสามตัว สนับสนุน Fault Tolerance แต่จะช้าเพราะต้องมาคำนวณ priority ว่าอะไรใช้ได้

RAID-10 : เอาความสามารถของ RAID-0 กับ RAID-1 มารวมกัน ต้องมีอย่างน้อย 4 ลูก A,B เป็น mirrors กัน C,D ด้วย AB, CD จะเป็น striping กัน

\* RAID ก็ยังจำเป้นต้องทำ back up

Fault tolerance Methods

Failover cluster เช่น DB server

load balancing เช่น web server

Trusted Recovery

การรับประกันว่าเมื่อเกิดความผิดพลาดขึ้น ระบบจะยังปลอดภัยเหมือนตอนก่อนเกิดความผิดพลาด

A fail- secure system : block ทุกการเข้าถึง

A fail-open system : ให้สิทธิ์ทุกการเข้าถึง เรียกอีกยอ่างว่า Fail-safe เป็นถ้าประตูที่ต้องสแกนบัตรจะเปิดให้คนหนีได้เองเมื่อเกิดไฟไหม้

four types of trusted recovery:

Manual Recovery

Automated Recovery

Automated Recovery without Undue Loss : มีกลไกบางอย่างที่ทำให้มั่นใจได้ว่า องค์ประกอบบางส่วนที่เฉพาะเจาะจงจะถูกป้องกันจากความสูญเสียได้ เช่น เก็บ transaction log นำมา rebuild ได้

Function Recovery ระบบสามารถย้อนกลับไปยังสถานะที่มัน มั่นคงอยู๋ได้

Quality of service (QoS)

Bandwidth

Latency

Jitter

Packet Loss ถ้าเยอะแสดงว่า QoS ต่ำ

Interference

\* ต้องหากลไกที่ทำให้ QoS สูงๆ

Recovery Strategy

DRP guides

Insurance จะจ่ายค่าเสียหายตามจริง ตามค่าเงินในช่วงนั้น

ไม่ใช่ทุกงานที่จะสำคัญ เช่น อาจจะกู้คืนมาเพียงแค่ 50%

Emergency Communications :ต้องมีการสื่อสารภายในเพื่อแก้ปัญหา รวมถึง สื่อสารไปยังภายนอกเพื่อให้ลูกค้าทราบว่าเรากำลังแก้ปัญหา หรือแก้ไขเรียบร้อยก็แจ้งลูกค้า

Alternate Processing Sites : ใช้เมื่อ site หลักไม่พร้อมที่จะใช้งาน

Cold Sites คือ ไม่มีอะไรเลย เป็นออฟฟิตเปล่าๆ อาจจะมีแค่สานโทรศัพท์ ข้อดีคือราคาถูก ข้อเสียคือ ใช้เวลามากเพื่อที่จะกลับมาให้บริการลูกค้าได้

Hot Sites : พร้อมที่จะให้พนักงานปฏิบัติหน้าที่ มีอะไรต่างๆ ที่เทียบเท่ากับ site หลัก

Warm Sites คือมี data link รวมถึงอุปกรณ์เครื่อง server เปล่าๆ ที่ทำให้สามารถให้บริการลูกค้าต่อได้ แต่จะไม่มี data ที่นี้ ต้องขนมาเอง ใช้เวลาประมาณ 12 ชั่วโมง ในการเตรียมความพร้อม

Mobile site : อยู่บนรถเคลื่อนที่สามารถที่จะทำงานได้เลย ส่วนใหญ่จะถูกตั้งให้เป็น Cold หรือ Warm

Service Bureau : บริษัทให้ให้เช่าคอมพิวเตอร์

Cloud Computing

Mutual assistance agreements (MAAs), also called reciprocal agreements คือ สองหน่วยงานเซ็นสัญญาร่วมกันว่าภ้าใครเกิดความผิดพลาดไปใช้อีกบริษัทหฯึ่งได้

Database Recovery (จัดเป็น Fault tolerance Methods)

Electronic Vaulting : ถ้าออกแบบจะใช้ site ผู้เชียวชาญก็จะไปดึง DB backup จาก Electronic Vault จากนั้นทำการส่งผ่านเครือข่าย ไปยัง Recovery site และก็ทำการติดตั้งไปยัง server (พูดง่ายๆก็คือ การทำ remote backup นานๆทำที)

Remote Journaling การทำ remote ทุกๆการเปลี่ยนแปลง ต่อยอดไปทีละนิด เอาไปเฉพาะตัวที่ไม่เคยเอาไป

Remote Mirroring : Real time มี sever สองเครื่องรันพร้อมกันแต่อยู่คนละ Site

Recovery Plan Development

Documents

Executive summary

Department-specific plans

Technical guides for IT personnel

Checklists for individuals on the disaster recovery team ว่าทำงานครบถ้วนไหม

Full copies of the plan มีเฉพาะสมาชิกที่เป็นระดับหัวหน้า

List of DRP team

Backups and Offsite Storage

Full Backups

Incremental Backups

Differential Backups

Backup Tape Formats

Disk-to-Disk Backup : back up ลง disk อีกลูก

Murphy’s law มันจะล่มก่อน backup วิธีป้องกันต้องใช้พวก RAID ช่วย หรือ remote mirroring

Tape Rotation : เอา tape กลับมาใช้ใหม่

hierarchical storage management (HSM) system เอา Tape มาต่อกันหลายๆ อันใช้ backup อย่างเดียว

Software Escrow Arrangements

ทำสัญญากับบริษัทที่ทำให้งานให้เรา เอา code ไปไว้ที่อื่น เมื่อบริษัทนั้นล่ม เราสามารถไปเรา code มาพัฒนาต่อได้ SLA จะเป็นตัวบอกให้ 3rd ส่ง code มาให้เรา

Recovery vs. Restoration

Recovery เกิดขึ้นที่ backup site โดย disaster recovery team ต้องกู้ให้ได้ภายในระยะเวลา MTD

Restoration เกิดขึ้นที่ primary site โดย salvage(กู้ภัย) team

Training, Awareness, and Documentation

DPR ต้องเป้นความลับและใช้คอรเซ็บ need to know

Testing and Maintenance

Read-Through Test อ่านอย่างเดียวเพื่อทบทวน

Structured Walk-Through : จะเรียกทีมมาประชุม เพื่อตัดสินว่าจะรับมือกับสถานการณ์ณ์ที่ยกตัวอย่างมาในที่ประชุมนั้นอย่างไร

Simulation Test : มีการประชุม และมีการดาว์นระบบลงเสมือยจริง

Parallel Test : จะมีการซ้อมอพยพบุคลากรไปยัง recovery site และทำกระบวกการ activate backup site ด้วย

Full-Interruption Test : ลอง shutdown ระบบ ที่ site หลักจริงๆ (ส่วนใหญ่ผู้บริหารไม่อนุญาตให้ทำ)

DRP จำเป็นต้องเปลี่ยน management เมื่อ infra change