QUẢN LÝ AN TOÀN THÔNG TIN

BÀI 3:
LẬP KẾ HOẠCH DỰ PHÒNG

MỤC TIÊU

- Thảo luận về nhu cầu lập kế hoạch dự phòng
- Mô tả các thành phần chính của lập kế hoạch dự phòng
- Xây dựng một bộ kế hoạch dự phòng đơn giản, sử dụng phân tích tác động kinh doanh
- Thảo luận về cách tổ chức sẽ chuẩn bị và thực hiện thử nghiệm các kế hoạch dự phòng
- Giải thích cách tiếp cận kế hoạch dự phòng thống nhất

Nguyên tắc quản lý an toàn thông tin

Các đặc điểm sau sẽ là trọng tâm của khóa học hiện tại (sáu chữ P):

1. Lập kế hoạch Chương 2 & 3
2. Chính sách Chương 4
3. Các chương trình
4. Sự bảo vệ
5. Con người
6. Quản lý dự án

http://csrc.nist.gov/publications/PubsTC.html

Giới thiệu

Một nghiên cứu cho thấy hơn 40% doanh nghiệp không có kế hoạch thảm họa phải ngừng hoạt động kinh doanh sau khi thua lỗ lớn

Phương pháp tiếp cận doanh nghiệp nhỏ

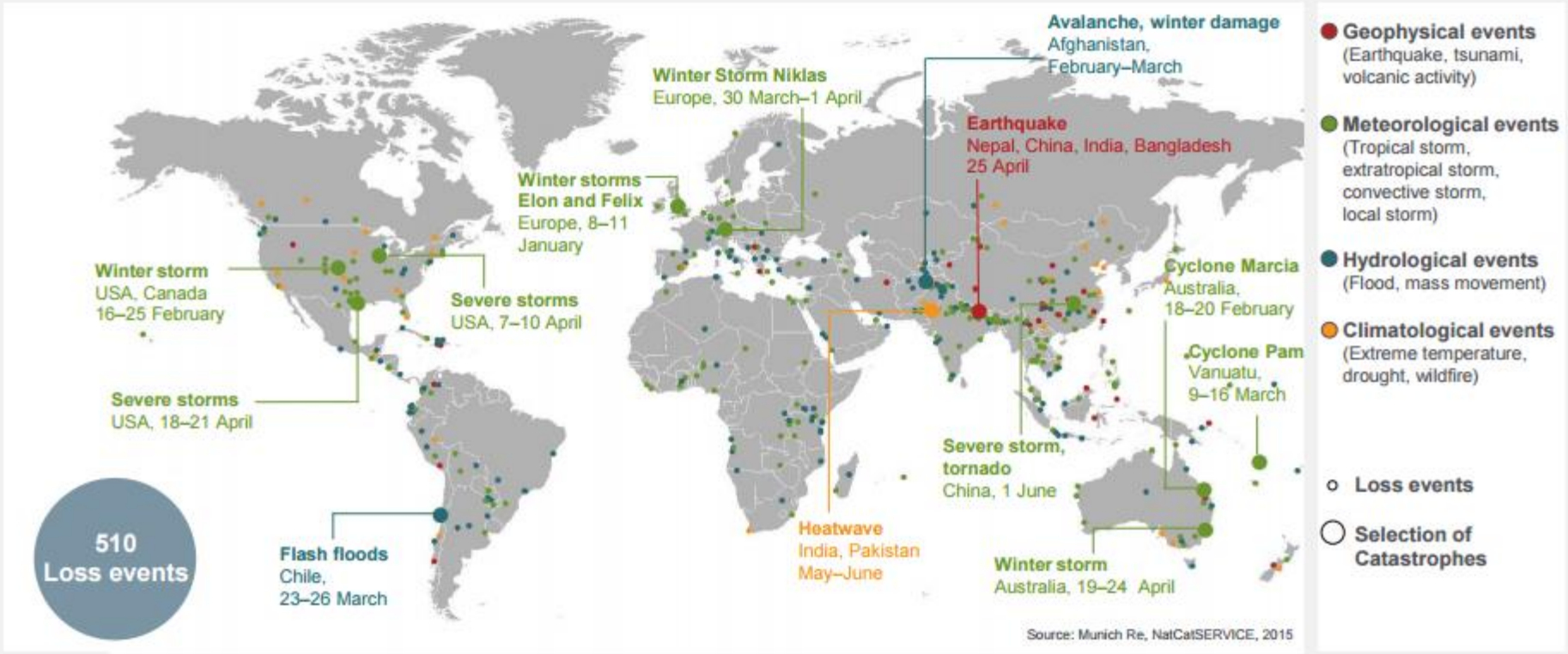
Phương pháp tiếp cận bổ sung

NatCatSERVICE

Loss events worldwide Jan – June 2015

Geographical overview

Munich RE

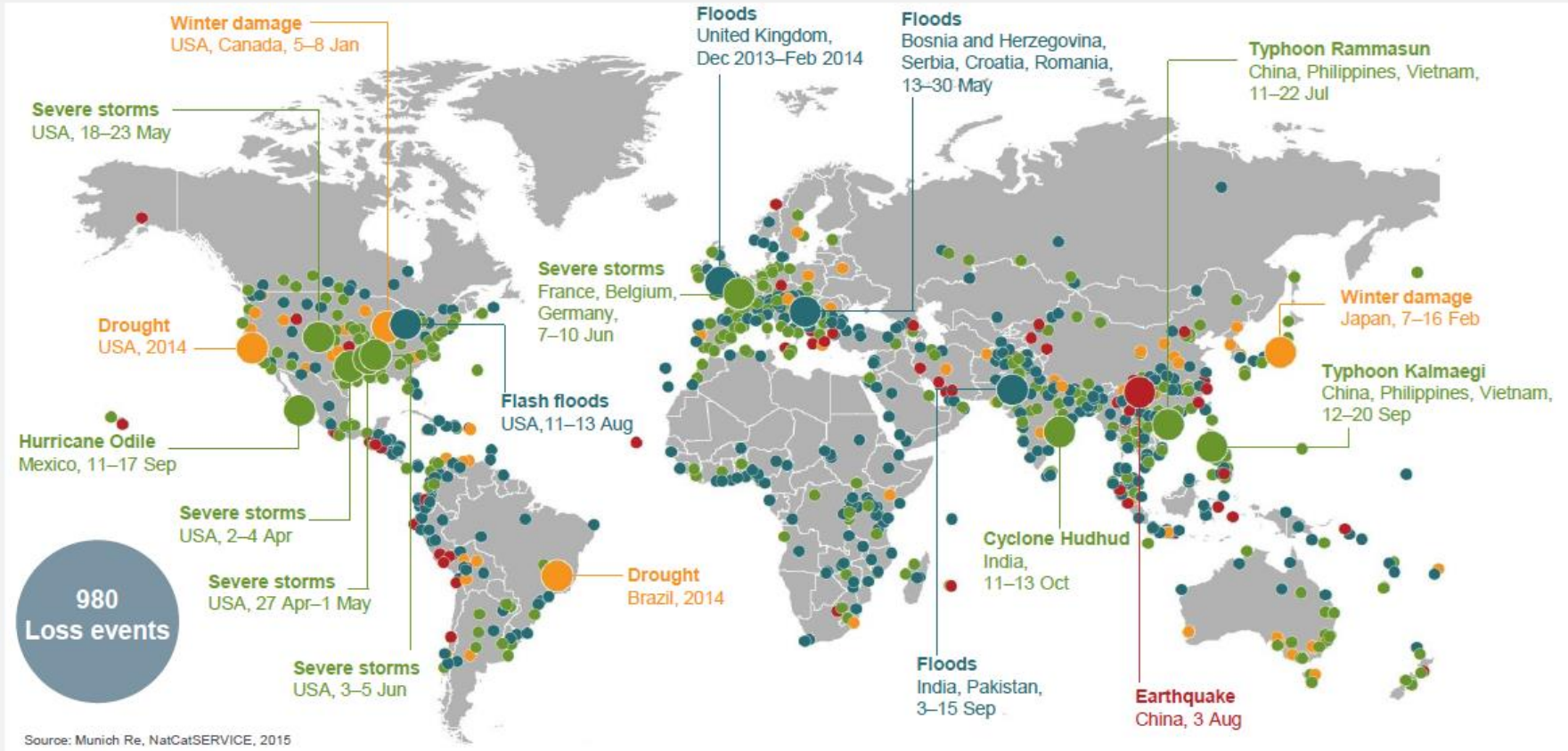


NatCatSERVICE

Loss events worldwide 2014

Geographical overview

Munich RE

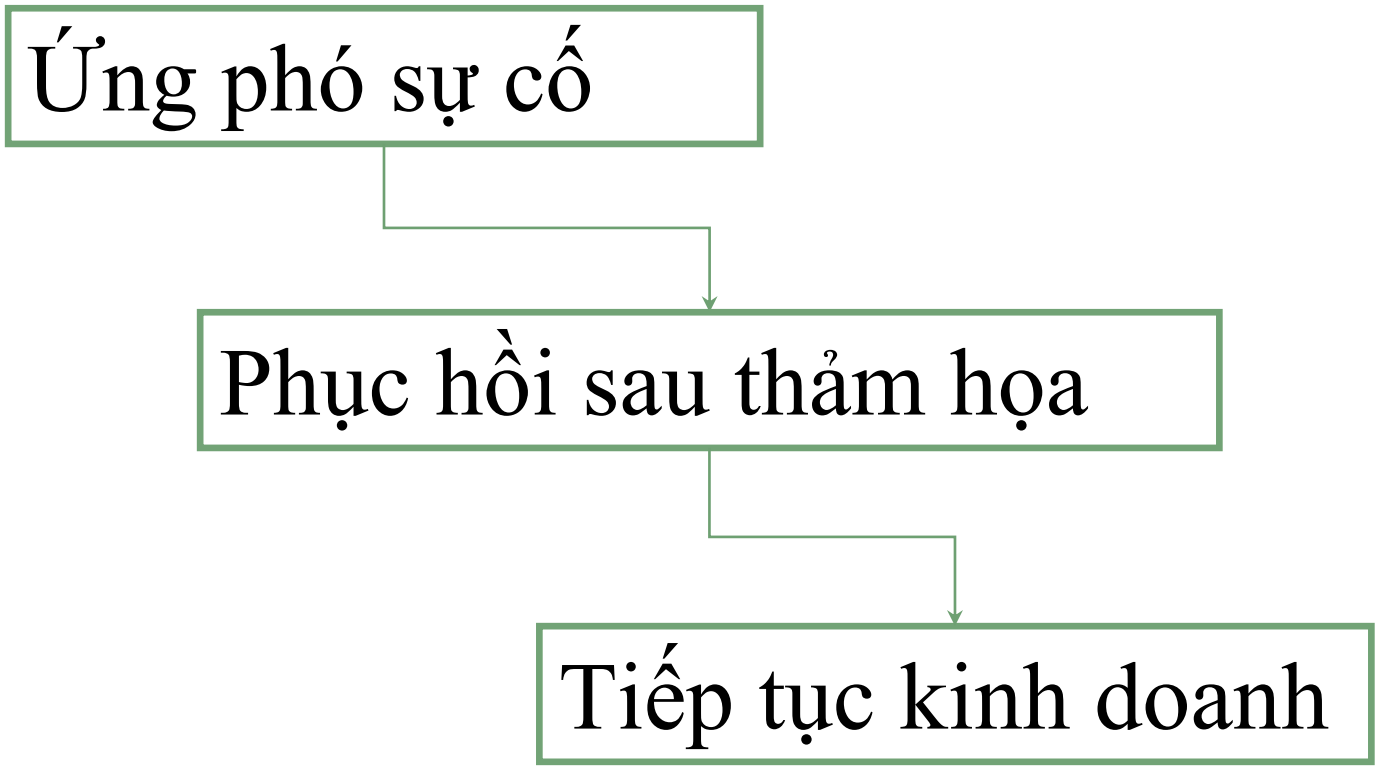


- **Loss events**
- **Selection of catastrophes**
  Overall losses ≥ US$ 1,500m
- **Geophysical events**
  (Earthquake, tsunami, volcanic activity)
- **Meteorological events**
  (Tropical storm, extratropical storm, convective storm, local storm)
- **Hydrological events**
  (Flood, mass movement)
- **Climatological events**
  (Extreme temperature, drought, wildfire)

Kế hoạch dự phòng

- Lập kế hoạch dự phòng (CP)
  - Lập kế hoạch tổng thể cho các sự kiện bất ngờ
  - Liên quan đến việc chuẩn bị, phát hiện, phản ứng và phục hồi sau các sự kiện đe dọa đến sự an toàn của tài nguyên và tài sản thông tin

Các nguyên tắc cơ bản về lập kế hoạch dự phòng

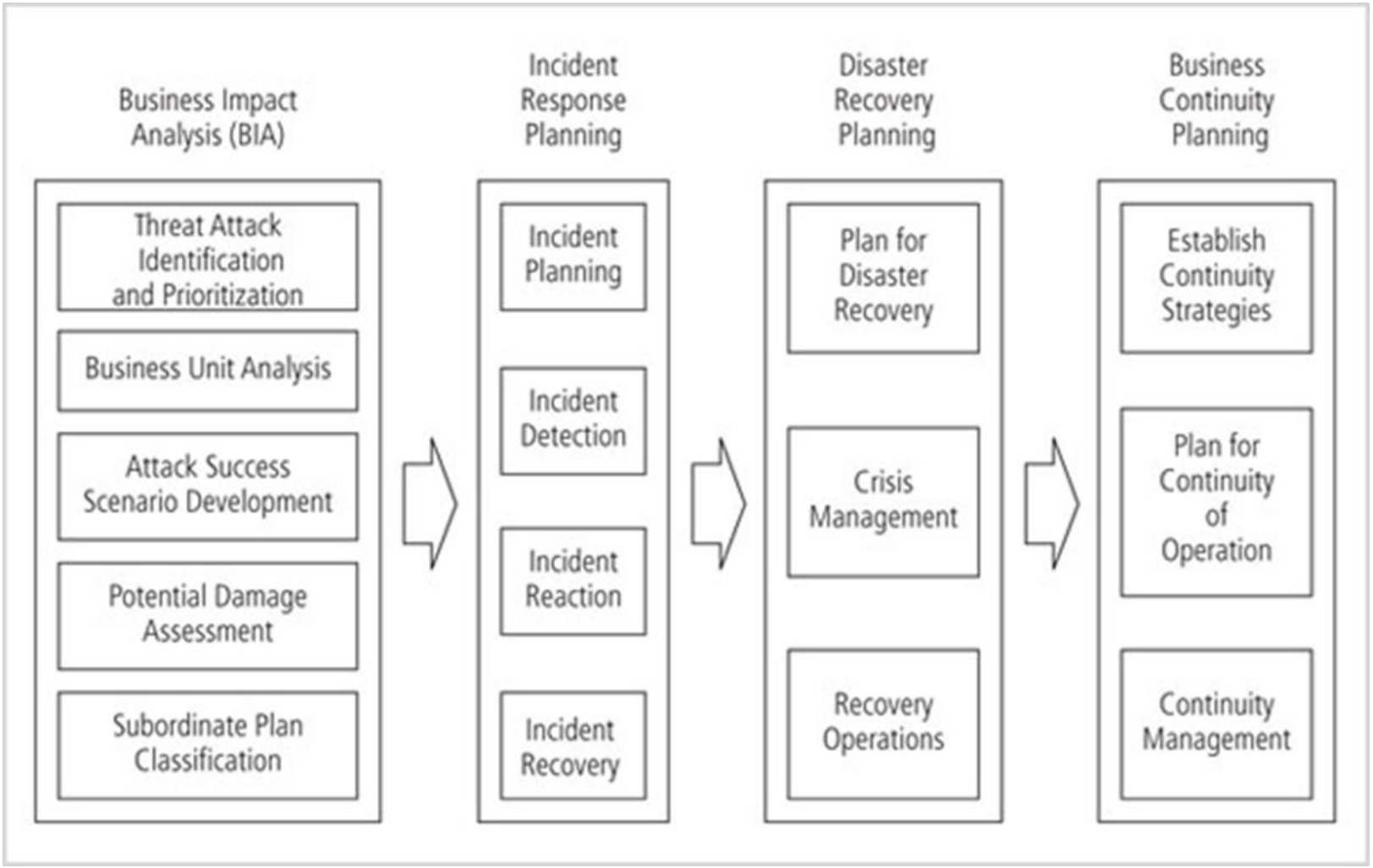


Xây dựng tài liệu CP

- Xây dựng tuyên bố chính sách lập kế hoạch dự phòng
- Tiến hành phân tích tác động kinh doanh (BIA - Business Impact Analysis)
- Xác định các biện pháp kiểm soát phòng ngừa
- Phát triển các chiến lược phục hồi
- Xây dựng kế hoạch dự phòng CNTT
- Lập kế hoạch kiểm tra, đào tạo và bài tập
- Lập kế hoạch bảo trì

Phân tích tác động kinh doanh (BIA)

Cung cấp các kịch bản chi tiết về tác động của từng cuộc tấn công tiềm tàng



Phân tích tác động kinh doanh (tiếp theo)

- Nhóm CP tiến hành BIA theo các giai đoạn sau:
  - Nhận dạng mối đe dọa tấn công
  - Phân tích đơn vị kinh doanh
  - Các tình huống tấn công thành công
  - Đánh giá thiệt hại tiềm tàng
  - Phân loại kế hoạch cấp dưới

- Các mục đích của BIA là gì?

Phân tích tác động kinh doanh (tiếp theo)

- Một tổ chức sử dụng quy trình quản lý rủi ro sẽ xác định và sắp xếp thứ tự ưu tiên cho các mối đe dọa

- Nhiệm vụ BIA chính thứ hai là phân tích và sắp xếp thứ tự ưu tiên cho các chức năng kinh doanh trong tổ chức
  - Mỗi loại nên được phân loại

Phân tích tác động kinh doanh (tiếp theo)

- Tạo một loạt các kịch bản mô tả tác động của cuộc tấn công thành công vào từng khu vực chức năng

- Hồ sơ tấn công nên bao gồm các tình huống mô tả cuộc tấn công điển hình bao gồm:

  (1) Phương pháp luận, (2) Các chỉ báo, (3) Hệ quả chung

- Ước tính chi phí

Việc này nên được thực hiện nội bộ hay thuê ngoài?

Quy trình kinh doanh của NIST và mức độ quan trọng của việc phục hồi

Các biện pháp phục hồi chính:

- Thời gian ngừng hoạt động tối đa có thể chịu đựng được (Maximum Tolerable Downtime-MTD) - tổng số thời gian mà chủ sở hữu hệ thống sẵn sàng chấp nhận cho một sứ mệnh/quy trình kinh doanh bị ngừng hoạt động hoặc gián đoạn

- Mục tiêu thời gian khôi phục (Recovery time objective-RTO) - thời gian tối đa mà tài nguyên hệ thống có thể không khả dụng trước khi có tác động không thể chấp nhận được đối với các quy trình và tài nguyên hệ thống khác

- Mục tiêu điểm khôi phục (Recovery point objective-RPO) - tại thời điểm, trước khi hệ thống bị gián đoạn hoặc ngừng hoạt động, dữ liệu của nhiệm vụ/quy trình kinh doanh có thể được khôi phục sau khi ngừng hoạt động

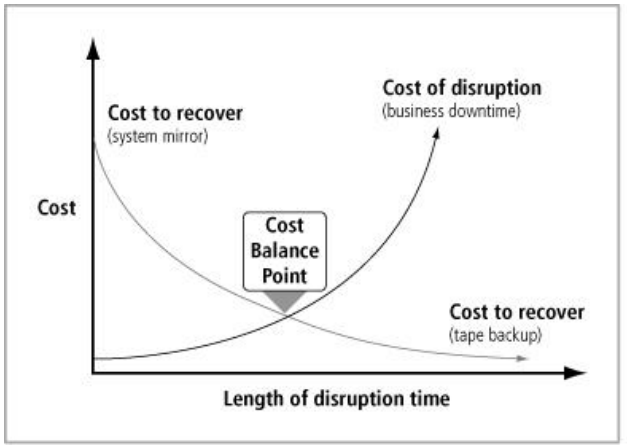
Quy trình kinh doanh của NIST và mức độ quan trọng của việc phục hồi

Thời gian khôi phục công việc (Work Recovery Time-WRT) - lượng nỗ lực cần thiết để chức năng kinh doanh hoạt động SAU KHI phần tử công nghệ được khôi phục

- Có thể được thêm vào RTO để xác định lượng thời gian thực tế đã trôi qua trước khi một chức năng kinh doanh trở lại hoạt động hữu ích

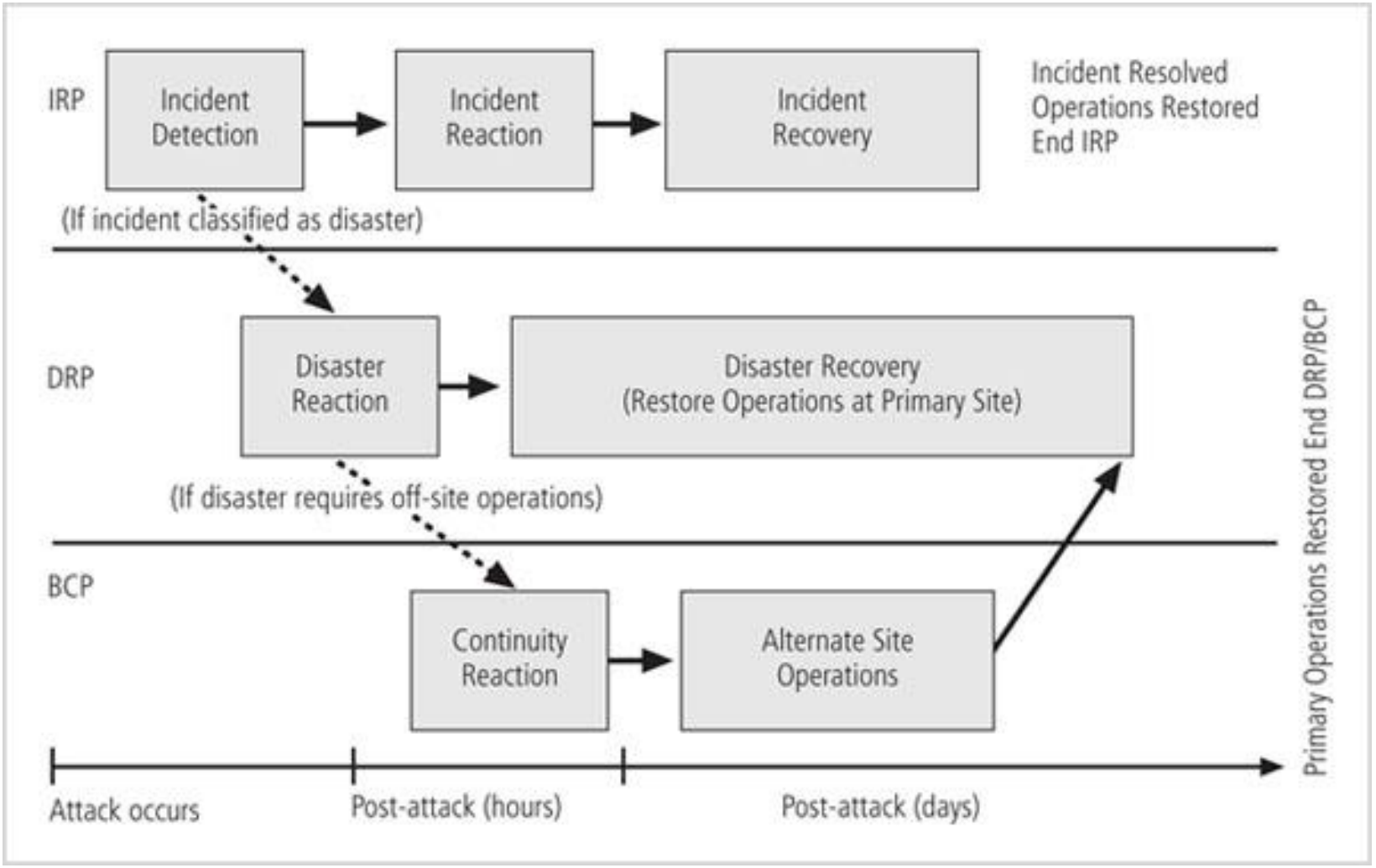
Tổng thời gian cần thiết để đưa chức năng kinh doanh hoạt động trở lại phải ngắn hơn Thời gian ngừng hoạt động tối đa có thể chịu đựng được - MTD

Phải cân bằng giữa chi phí hệ thống không hoạt động với chi phí khôi phục



Date of analysis:	June 23, 2011
Attack name/description:	*Malicious code via e-mail*
Threat/probable threat agents:	• *Vandalism/script kiddies* • *Theft/experienced hacker*
Known or possible vulnerabilities:	• *Emergent weakness in e-mail clients* • *Inappropriate actions by employees, contractors, and visitors using e-mail clients* • *Emergent weakness in e-mail servers or gateways*
Likely precursor activities or indicators:	*Announcements from vendors and bulletins*
Likely attack activities or indicators of attack in progress:	• *E-mail volume measurements may show variances* • *Unusual system failures among clients* • *Unusual system failures among servers* • *Notification from e-mail recipients who may be ahead of us in attack life cycle*
Information assets at risk from this attack:	*All connected systems due to blended attack model now prevalent*
Damage or loss to information assets likely from this attack:	• *Denial-of-service for some clients almost certain* • *Denial-of-service for servers possible* • *Possible losses of data depending on nature of attack*
Other assets at risk from this attack:	*None likely*
Damage or loss to other assets likely from this attack:	*None likely*
Immediate actions indicated when this attack is under way:	• *Disconnect e-mail gateway(s)* • *Update e-mail gateway filtering patterns and apply* • *Update and distribute client filtering patterns* • *Isolate all infected servers* • *Isolate all infected clients* • *Begin server recovery actions for infected servers* • *Begin client recovery actions for infected clients*
Follow-up actions after this attack was successfully executed against our systems:	*Review pattern update timing and procedure to assure adequacy*
Comments:	*None at this time*

Thời gian và trình tự của các phần tử CP



Kế hoạch ứng phó sự cố

Câu hỏi đặt ra là sẽ không xảy ra sự cố,
nhưng đúng hơn là khi một sự cố sẽ xảy ra

- Một tập hợp chi tiết các quy trình và thủ tục bắt đầu khi sự cố được phát hiện

- Khi một mối đe dọa trở thành một cuộc tấn công thực sự, nó được phân loại là một sự cố an toàn thông tin nếu nó:
  - chống lại tài sản thông tin
  - có cơ hội thành công trong thực tế
  - đe dọa tính bảo mật, tính toàn vẹn hoặc tính sẵn có của các tài sản thông tin

Kế hoạch ứng phó sự cố (tiếp theo)

Ai là người tạo ra kế hoạch ứng phó sự cố?

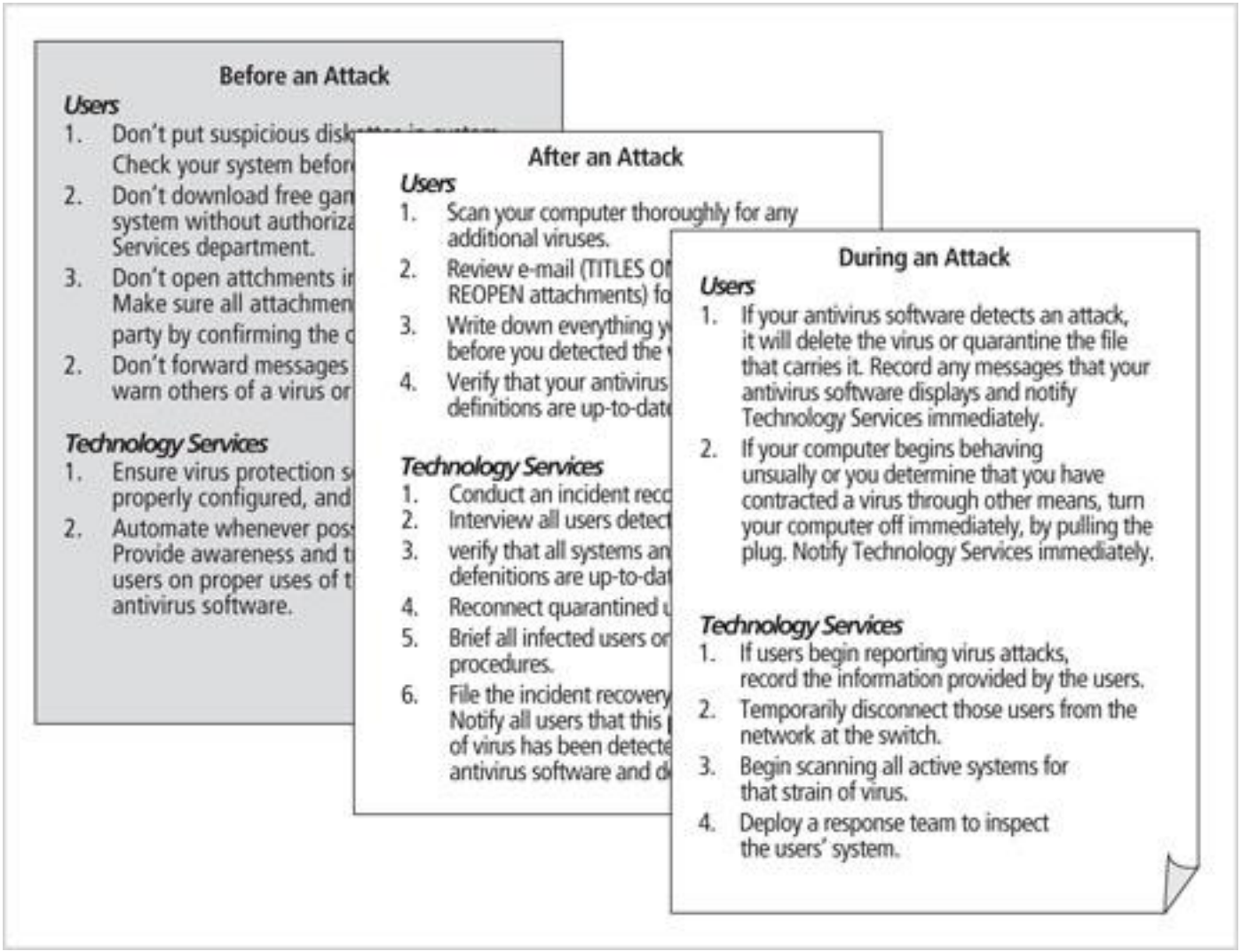
- Những người lập kế hoạch xây dựng và viết các thủ tục nhằm thực hiện **khi** sự cố xảy ra và **ngay sau** khi sự cố chấm dứt

- Các vùng chức năng riêng biệt có thể xây dựng các thủ tục khác nhau

Kế hoạch ứng phó sự cố (tiếp theo)

- Xây dựng quy trình cho các nhiệm vụ phải thực hiện trước khi xảy ra sự cố
  - Chi tiết về lịch trình sao lưu dữ liệu
  - Chuẩn bị phục hồi sau thảm họa
  - Lịch đào tạo
  - Kế hoạch kiểm tra
  - Bản sao của các thỏa thuận dịch vụ
  - Kế hoạch kinh doanh liên tục

Kế hoạch ứng phó sự cố (tiếp theo)



Kế hoạch ứng phó sự cố (tiếp theo)

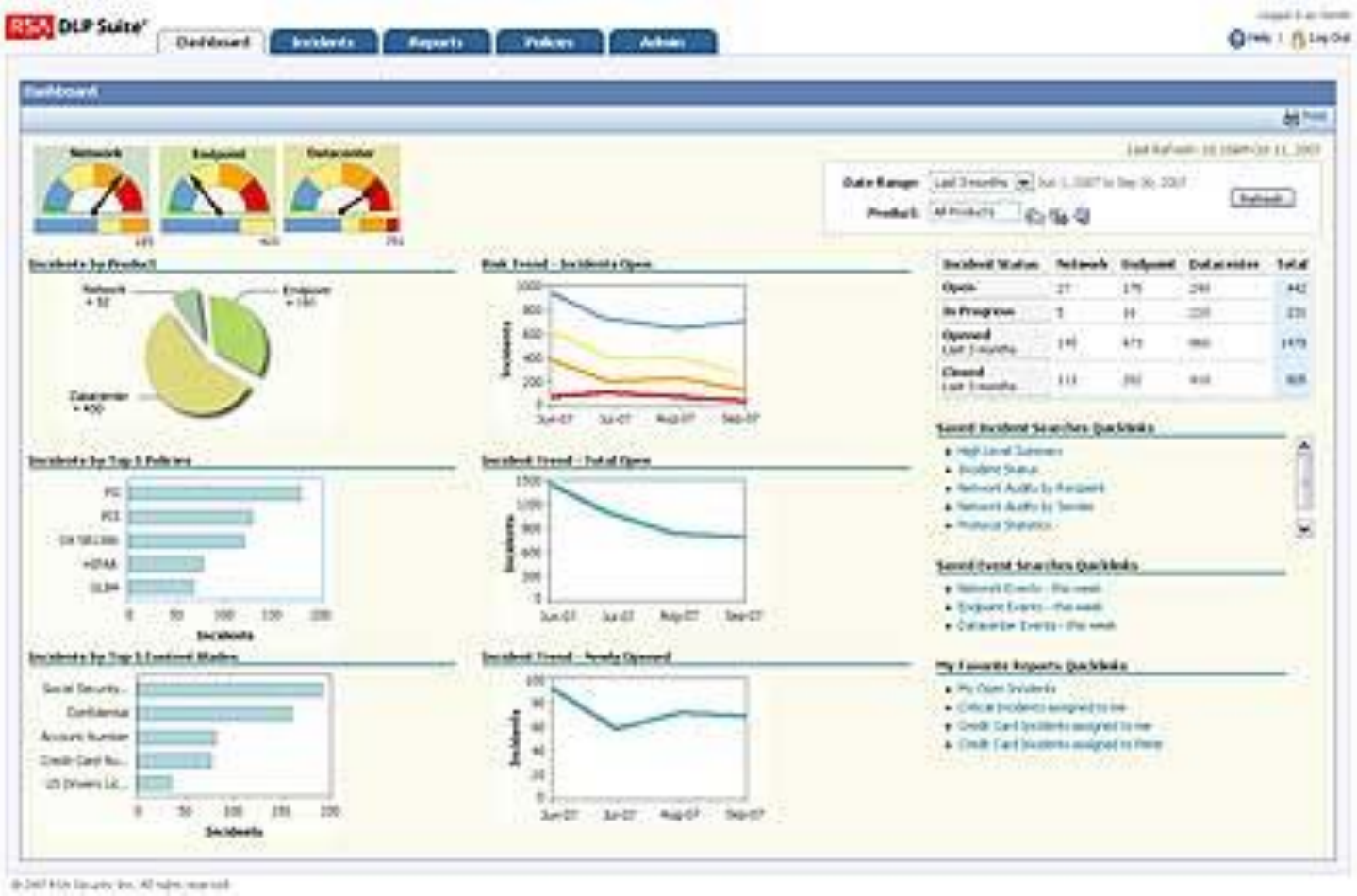
- Lập kế hoạch đòi hỏi sự hiểu biết chi tiết về các hệ thống thông tin và các mối đe dọa mà chúng phải đối mặt

- Nhóm lập kế hoạch ứng phó sự cố tìm cách xây dựng các phản hồi được xác định trước để hướng dẫn người dùng thông qua các bước cần thiết nhằm ứng phó với một sự cố

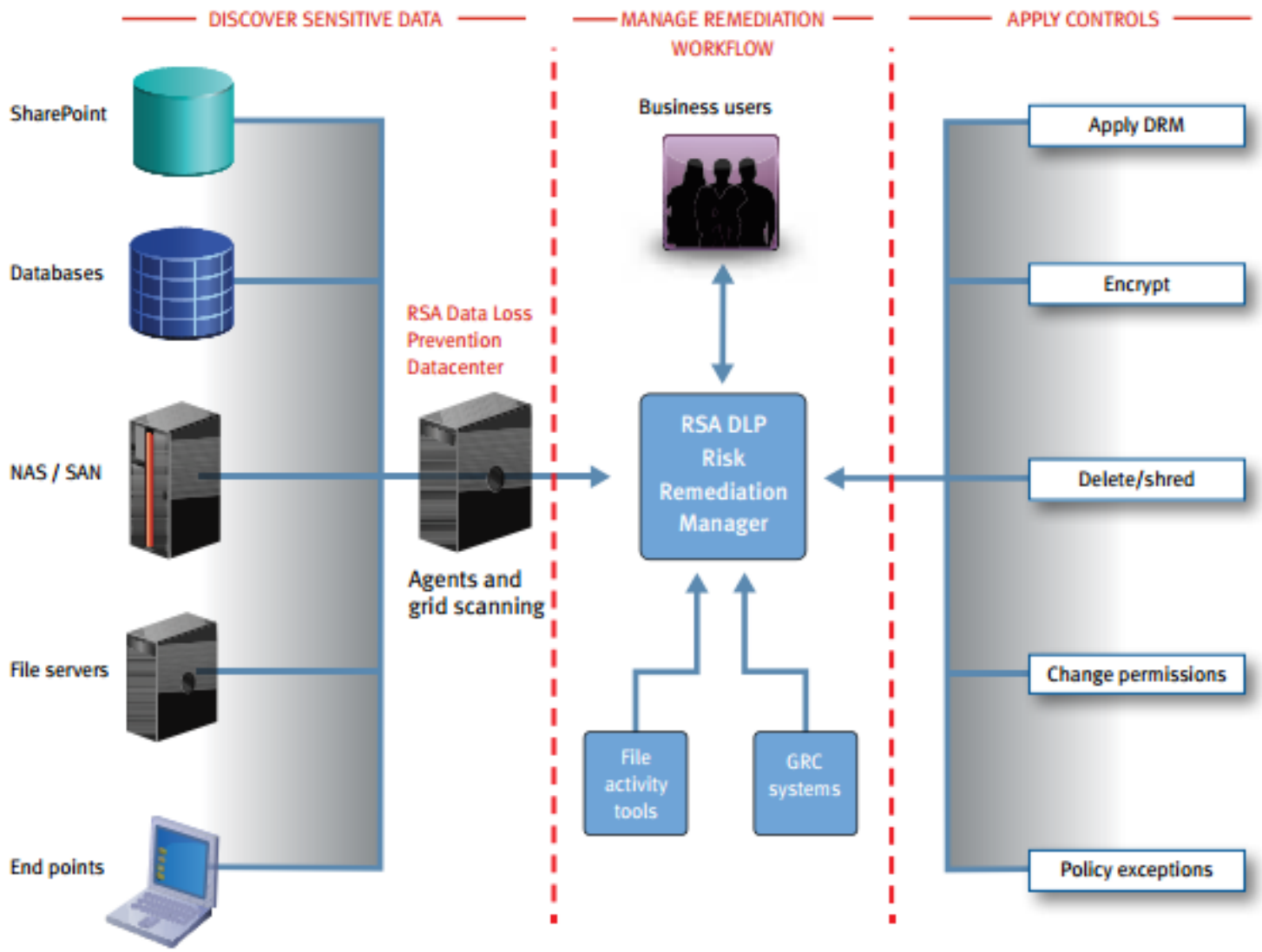
Kế hoạch ứng phó sự cố (tiếp theo)

- Phân loại sự cố
  - Xác định xem một sự kiện có phải là một sự cố thực sự hay không
  - Sử dụng các báo cáo ban đầu từ người dùng cuối, hệ thống phát hiện xâm nhập, phần mềm phát hiện vi rút dựa trên máy chủ và mạng cũng như quản trị viên hệ thống
    (Ví dụ: Ngăn chặn việc mất mát dữ liệu RSA)

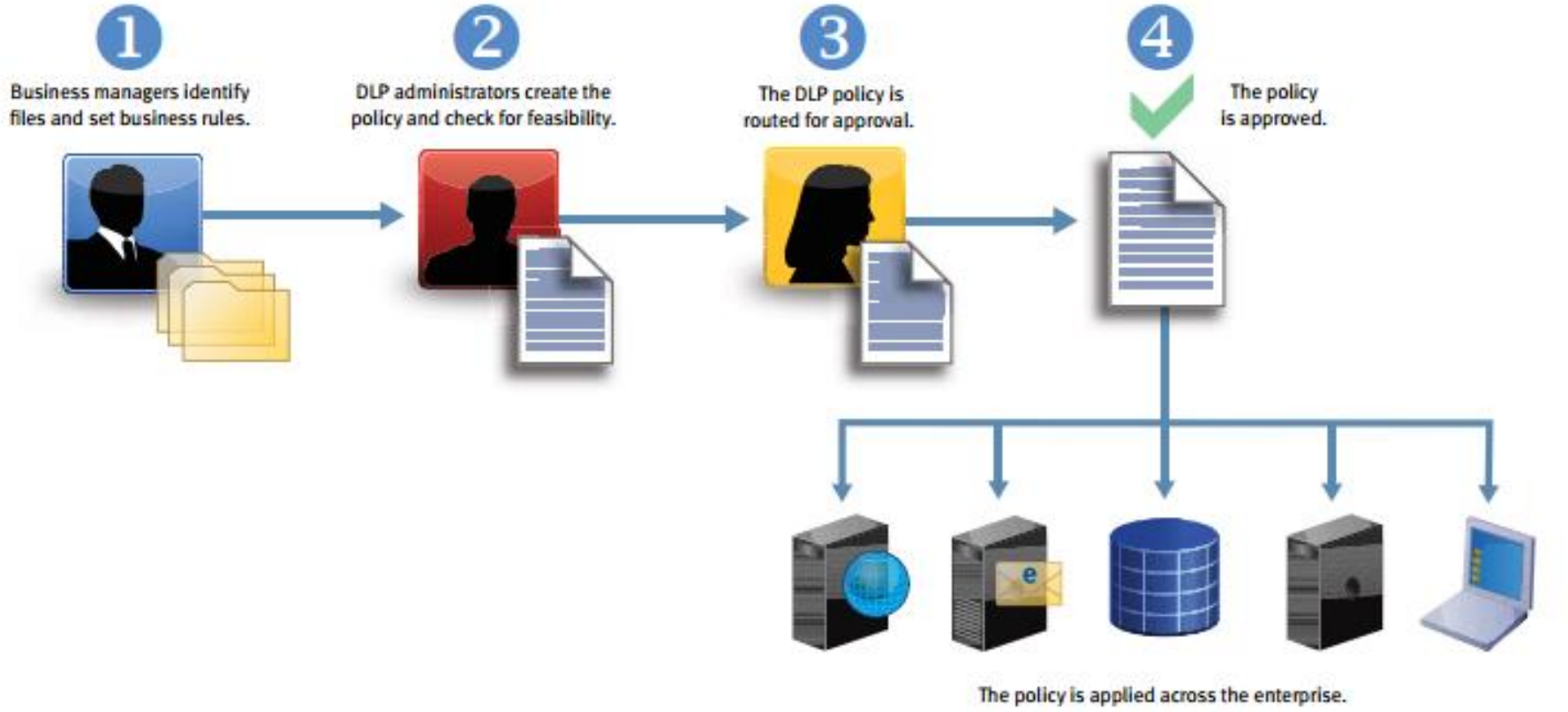
Phần mềm ứng phó sự cố



Công cụ lập kế hoạch ứng phó sự cố



Công cụ lập kế hoạch ứng phó sự cố



Kế hoạch ứng phó sự cố: Các chỉ báo

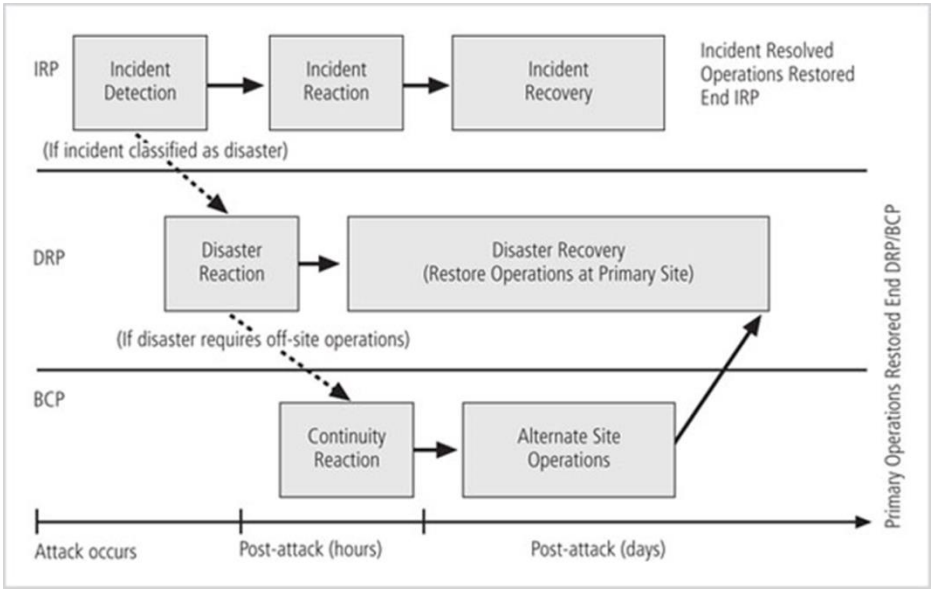
- **Các chỉ báo khả thi**
- **Các chỉ báo xác suất**
- **Các chỉ báo xác định**

- Khi những điều sau đây xảy ra, ứng phó sự cố tương ứng phải được kích hoạt ngay lập tức
  - Mất khả năng cung cấp
  - Mất tính toàn vẹn
  - Mất tính bí mật
  - Vi phạm chính sách
  - Vi phạm pháp luật

http://www.npr.org/blogs/thetwo-way/2013/01/16/169528579/outsourced-employee-sends-own-job-to-china-surfs-web

Kế hoạch ứng phó sự cố (tiếp theo)

- Sau khi một sự cố thực tế đã được xác nhận và phân loại đúng
  - Nhóm IR chuyển từ giai đoạn phát hiện sang giai đoạn phản ứng
  - Một số bước hành động phải diễn ra nhanh chóng và có thể xảy ra đồng thời



Kế hoạch ứng phó sự cố: Các bước hành động

1. Thông báo về nhân sự chủ chốt (danh sách cảnh báo)

1. Phân công nhiệm vụ

1. Tài liệu về vụ việc

Kế hoạch ứng phó sự cố (tiếp theo)

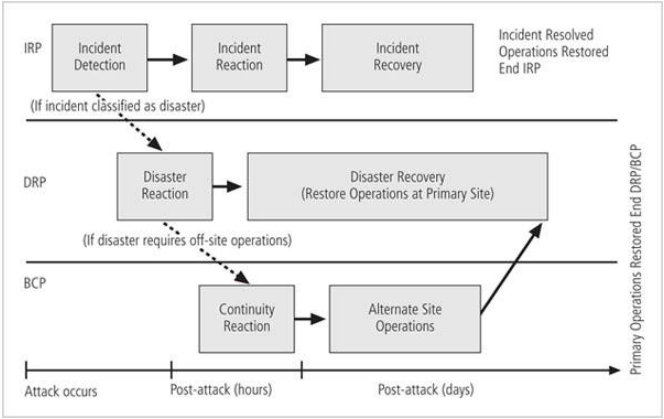
- Nhiệm vụ thiết yếu của ứng phó sự cố là ngăn chặn sự cố hoặc ngăn chặn tác động của nó

- Các chiến lược ngăn chặn sự cố tập trung vào hai nhiệm vụ:

IRP: Ngăn chặn sự cố

Các chiến lược ngăn chặn

- Sau khi kiểm soát hệ thống được kiểm soát và lấy lại, quá trình khôi phục sự cố có thể bắt đầu
- Đánh giá thiệt hại sự cố
- Sự cố có thể tăng về phạm vi hoặc mức độ nghiêm trọng đến mức IRP không thể ngăn chặn sự cố một cách đầy đủ



IRP: Quy trình phục hồi

- Xác định các lỗ hổng
- Giải quyết các biện pháp bảo vệ không thành công
- Đánh giá khả năng giám sát (nếu có)
- Khôi phục dữ liệu từ các bản sao lưu nếu cần
- Khôi phục các dịch vụ và quy trình đang sử dụng
- Liên tục giám sát hệ thống
- Khôi phục sự tự tin của các thành viên

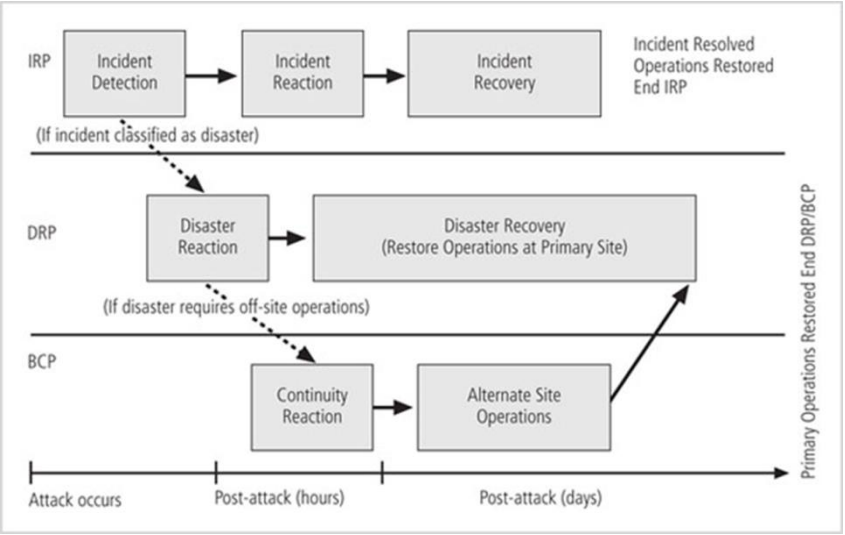
Kế hoạch ứng phó sự cố (tiếp theo)

- Khi một sự cố vi phạm luật dân sự hoặc hình sự, tổ chức có trách nhiệm thông báo cho các cơ quan có thẩm quyền thích hợp
  - Sử dụng công cụ luật pháp có cả lợi thế và bất lợi

Kế hoạch khôi phục sau thảm họa

- Chuẩn bị và phục hồi sau thảm họa, dù là do tự nhiên hay do con người tạo ra

- Nói chung, một sự cố là một thảm họa khi:



Kế hoạch khôi phục sau thảm họa (tiếp theo)

- Vai trò quan trọng của (Disaster Recovery Plan-DRP) là xác định cách thiết lập lại hoạt động tại vị trí mà tổ chức thường đặt

- Các phân loại DRP phổ biến:
  - Thảm họa thiên nhiên
  - Thảm họa do con người tạo ra

- Phát triển kịch bản và phân tích tác động
  - Được sử dụng để phân loại mức độ đe dọa của từng thảm họa tiềm ẩn

Kế hoạch khôi phục sau thảm họa (tiếp theo)

Thảo luận về những lầm tưởng về khôi phục sau thảm họa

Xua tan 10 lầm tưởng về khôi phục thảm họa phổ biến: Bài học rút ra từ cơn bão Katrina và các thảm họa khác

BRETT J. L. LANDRY
Đại học Dallas
VÀ
M. SCOTT KOGER
Đại học Western Carolina


Our Disaster Recovery Plan
Goes Something Like This...
HELP!
HELP!
DILBERT
By Scott Adams

Những lầm tưởng phổ biến cần tránh khi khắc phục thảm họa

- Chỉ có 1 kế hoạch duy nhất cho các thảm họa tự nhiên
- Thử nghiệm giả là không đủ
- Các mối đe dọa bên ngoài là cuộc tấn công duy nhất vào tài nguyên
- Các địa điểm khôi phục dữ liệu đã sẵn sàng cho khắc phục thảm họa
- Các khu vực không làm việc của nhân viên được trang bị đầy đủ

Những lầm tưởng phổ biến cần tránh khi khắc phục thảm họa

- Triển khai thử nghiệm khắc phục thảm họa ở một thời điểm muộn hơn cho các hệ thống mới
- Thiết bị thay thế sẽ có sẵn cho khắc phục thảm họa Trong hoặc Sau
- Dữ liệu sao lưu Hoạt động và có thể được Khôi phục sau khắc phục thảm họa
- Khắc phục thảm họa có thể được lập kế hoạch trong Kho công ty.
- Nhân viên nhận thức được những gì họ cần phải làm

Phục hồi sau thảm họa

- Hãy là một 'Người bi quan' - (Chương trình truyền hình Doomdayers)
- Lập kế hoạch, lập kế hoạch và lập kế hoạch
- Nhiều tình huống
- Có nhiều bản sao lưu và dự phòng
- Kiểm tra - Đã lên lịch và Không theo lịch trình
- Giữ cho việc lập kế hoạch và chuẩn bị khắc phục thảm họa như một nhiệm vụ liên tục

Ngoài bài viết

- Nhiều nhà cung cấp trợ giúp với Kế hoạch khắc phục thảm họa
- Tập hợp một Nhóm khắc phục thảm họa
- Ghi lại mọi thứ đã có sách hướng dẫn
- Kinh nghiệm cá nhân

https://www-01.ibm.com/support/knowledgecenter/ssw_ibm_i_71/rzarm/rzarmdisastr.htm
http://www.sungardas.com/Documents/disaster-recovery-plan-template-SFW-WPS-086.pdf
http://www.disasterrecovery.org/plan_steps.html

Kế hoạch khôi phục sau thảm họa (tiếp theo)

Thảo luận về danh sách kiểm tra khôi phục sau thảm họa

Kế hoạch liên tục kinh doanh
(Business Continuity Plan-BCP)

- Đảm bảo các chức năng kinh doanh quan trọng có thể tiếp tục trong một thảm họa
- Được kích hoạt và thực thi đồng thời với Kế hoạch khôi phục sau thảm họa khi cần thiết
- Phụ thuộc vào việc xác định các chức năng kinh doanh quan trọng và các nguồn lực để hỗ trợ chúng

BCP: Chiến lược

Các chiến lược liên tục

Kế hoạch liên tục kinh doanh: Tùy chọn địa điểm

- Hot site
- Warm site
- Cold site

- Các giải pháp thay thế khác: Chia sẻ thời gian, Phòng dịch vụ, Thỏa thuận chung

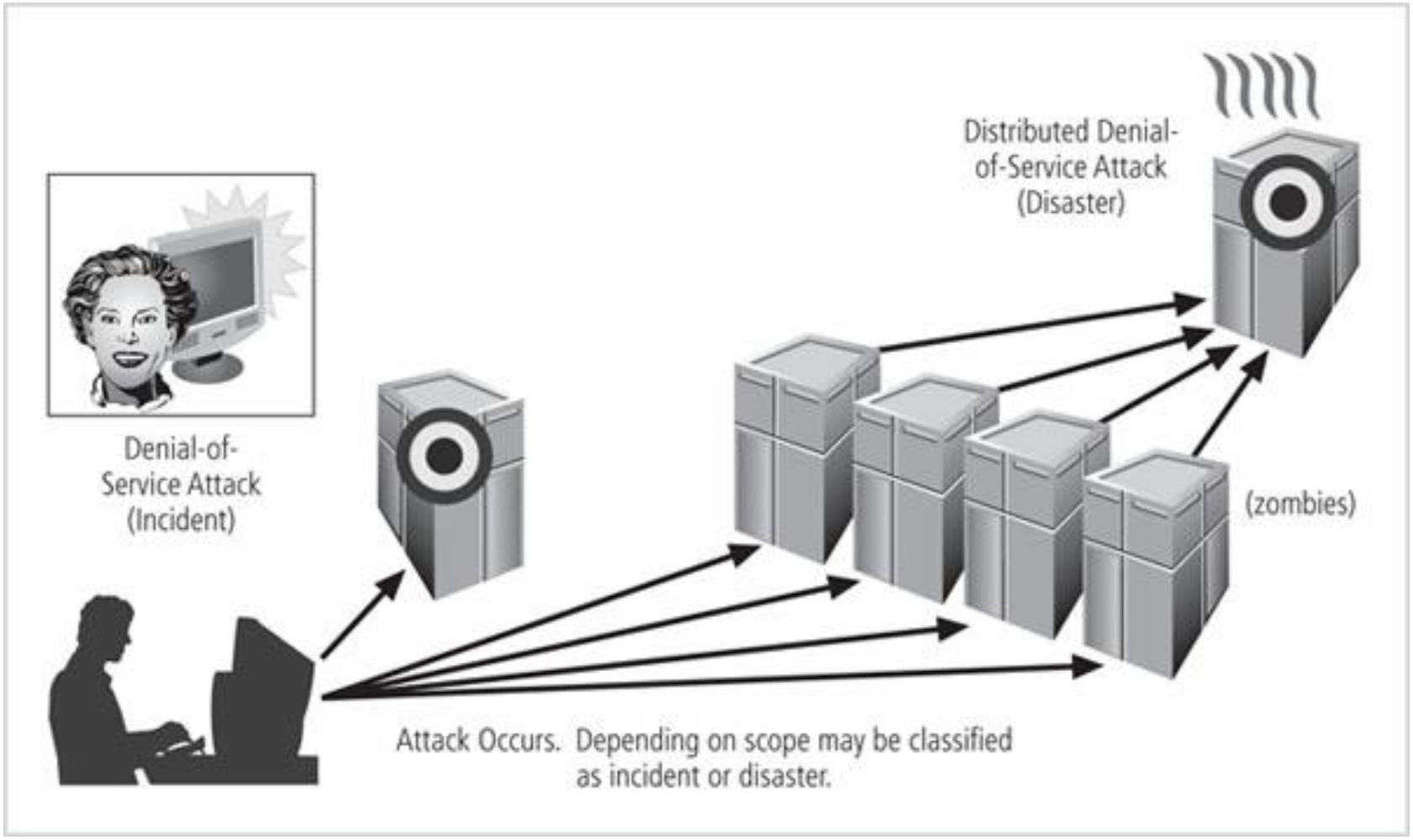
Ví dụ: Trung tâm dữ liệu RSA - thuê đường dây Ethernet 2 - 10gig giữa MA và NC

Kế hoạch liên tục kinh doanh (tiếp theo)

- Để bất kỳ site BCP nào hoạt động nhanh chóng, tổ chức phải có khả năng khôi phục dữ liệu

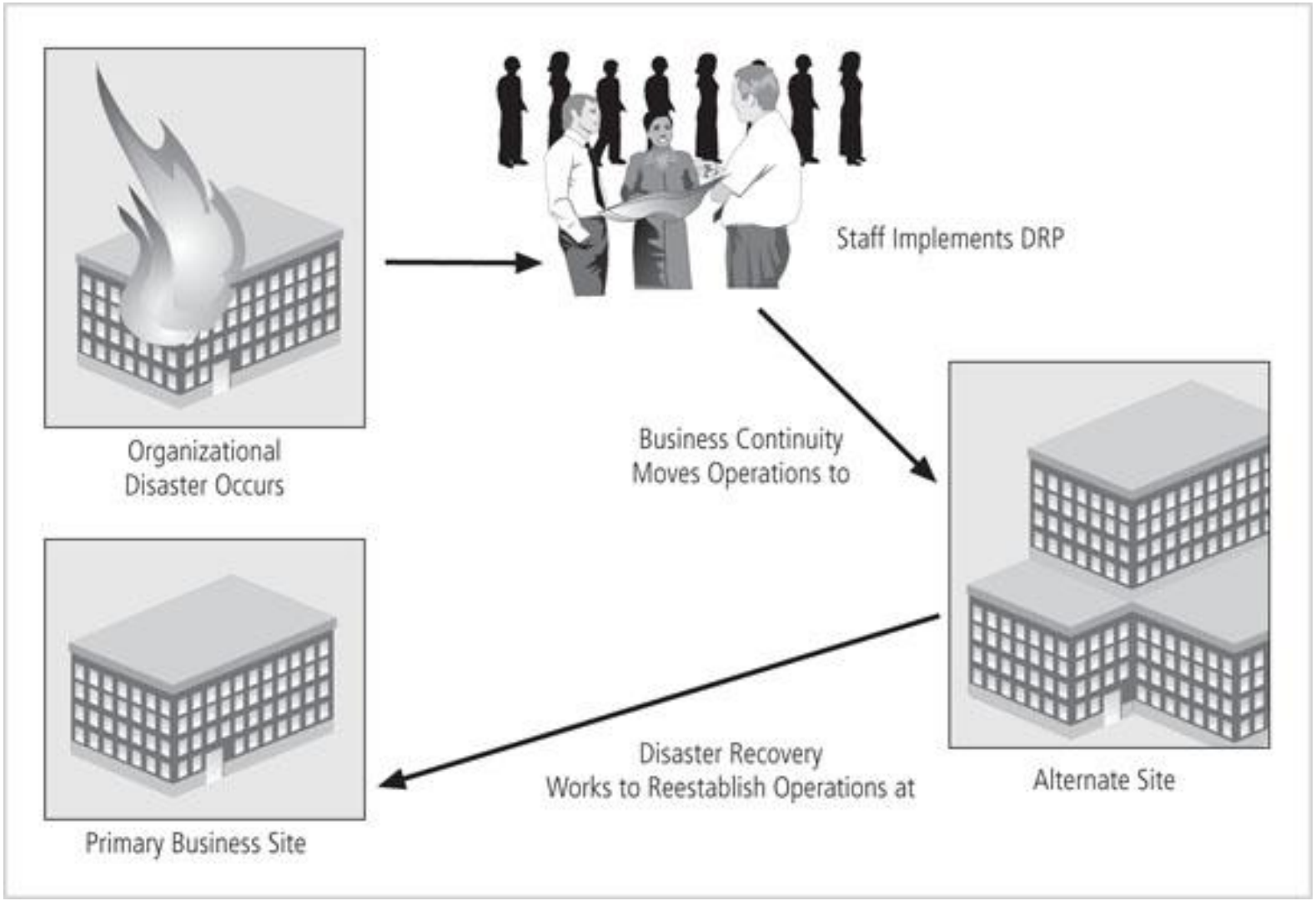
- Các tùy chọn bao gồm:

Thời gian và trình tự của các phần tử CP

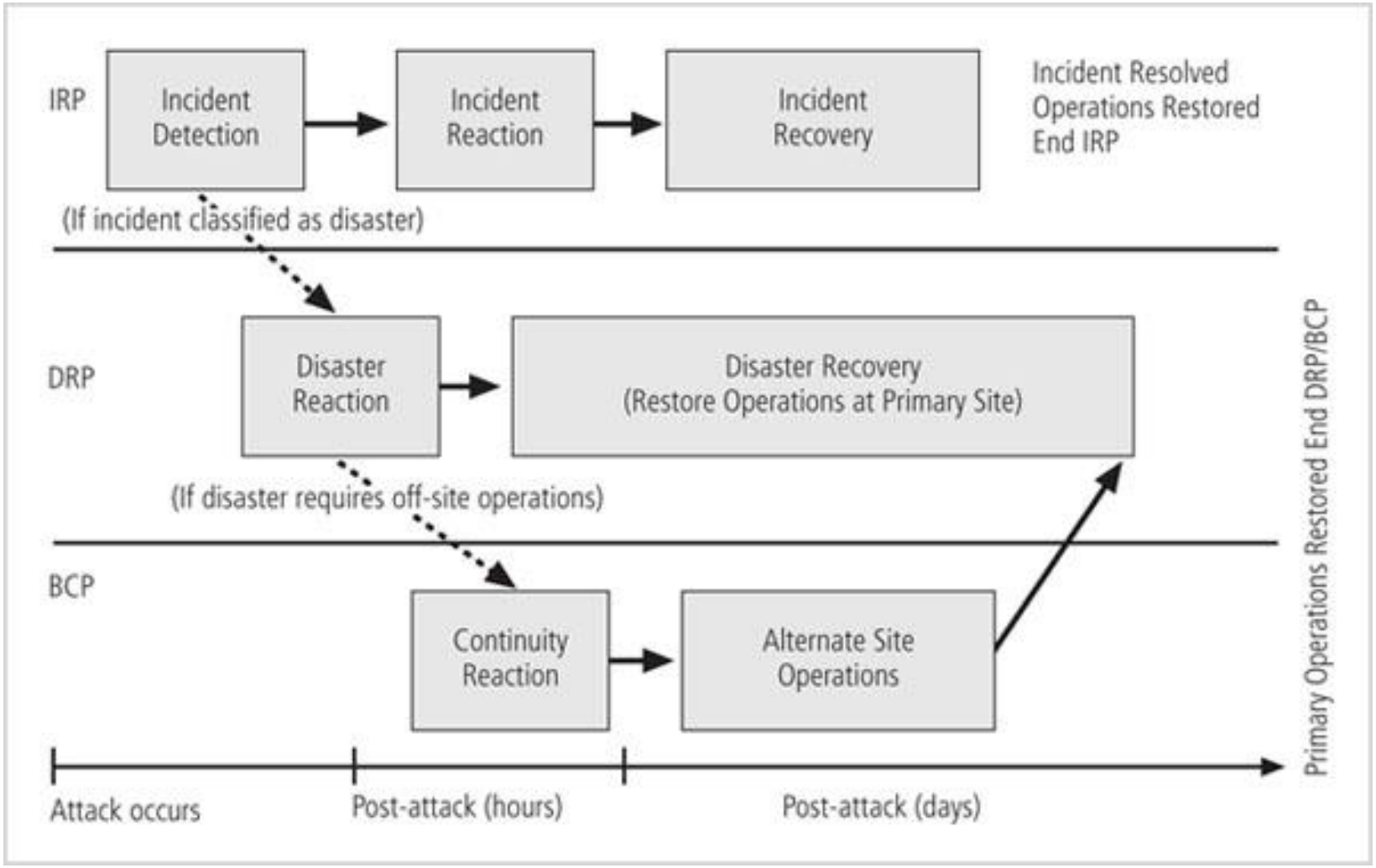


Hình 3-4 Ứng phó sự cố và khắc phục hậu quả thiên tai

Thời gian và trình tự của BCP



Thời gian và trình tự của các phần tử CP



Lập kế hoạch tiếp tục kinh doanh

- Bởi vì DRP và BCP có liên quan chặt chẽ với nhau, hầu hết các tổ chức chuẩn bị chúng đồng thời

Lập kế hoạch tiếp tục kinh doanh (tiếp theo)

- Các thành phần của một kế hoạch khôi phục thảm họa đơn giản
  - Tên cơ quan
  - Ngày hoàn thành hoặc cập nhật kế hoạch và ngày kiểm tra
  - Nhân viên sẽ được gọi trong trường hợp xảy ra thảm họa
  - Dịch vụ khẩn cấp sẽ được gọi (nếu cần) trong trường hợp xảy ra thảm họa

Lập kế hoạch tiếp tục kinh doanh (tiếp theo)

- Các thành phần của một kế hoạch khôi phục thảm họa đơn giản (tiếp theo)
  - Vị trí của thiết bị và vật tư khẩn cấp bên trong
  - Nguồn cung cấp thiết bị bên ngoài công trường
  - Danh sách ưu tiên cứu hộ
  - Quy trình khắc phục thảm họa của cơ quan
  - Đánh giá tiếp theo

Kiểm tra kế hoạch dự phòng

- Các vấn đề được xác định trong quá trình thử nghiệm
  - Các cải tiến có thể được thực hiện, để có được một kế hoạch đáng tin cậy

- Các chiến lược kiểm tra kế hoạch dự phòng
  - Một người kiểm tra
  - Hướng dẫn có cấu trúc
  - Mô phỏng
  - Thử nghiệm song song
  - Kiểm tra toàn bộ gián đoạn

Lập kế hoạch dự phòng: Những suy nghĩ cuối cùng

- Lặp lại dẫn đến cải thiện
- Việc thực hiện chính thức phương pháp luận này là một quá trình được gọi là cải tiến quy trình liên tục (CPI)
- Mỗi khi kế hoạch được diễn tập, nó phải được cải thiện
- Đánh giá và cải tiến liên tục dẫn đến kết quả được cải thiện

Kết chương

Bài tập

TÌm thông tin trên các trang web của công ty nào có kế hoạch ứng phó sự cố, phục hồi sau thảm họa và đảm bảo kinh doanh liên tục. Ưu tiên tại Việt Nam.