CHƯƠNG 06

XÂY DỰNG KẾ HOẠCH DỰ PHÒNG

Chương 06 - MỤC TIÊU

- Nắm được về xây dựng kế hoạch dự phòng, quy trình xây dựng kế hoạch dự phòng, các thành phần chính của kế hoạch dự phòng, kiểm tra kế hoạch dự phòng.

XÂY DỰNG KẾ HOẠCH DỰ PHÒNG

- Kế hoạch dự phòng
- Ứng cứu sự cố
- Khắc phục thảm họa
- Tính liên tục nghiệp vụ
- Quản lý khủng hoảng
- Kiểm tra kế hoạch dự phòng
- Câu hỏi ôn tập

Kế hoạch dự phòng…

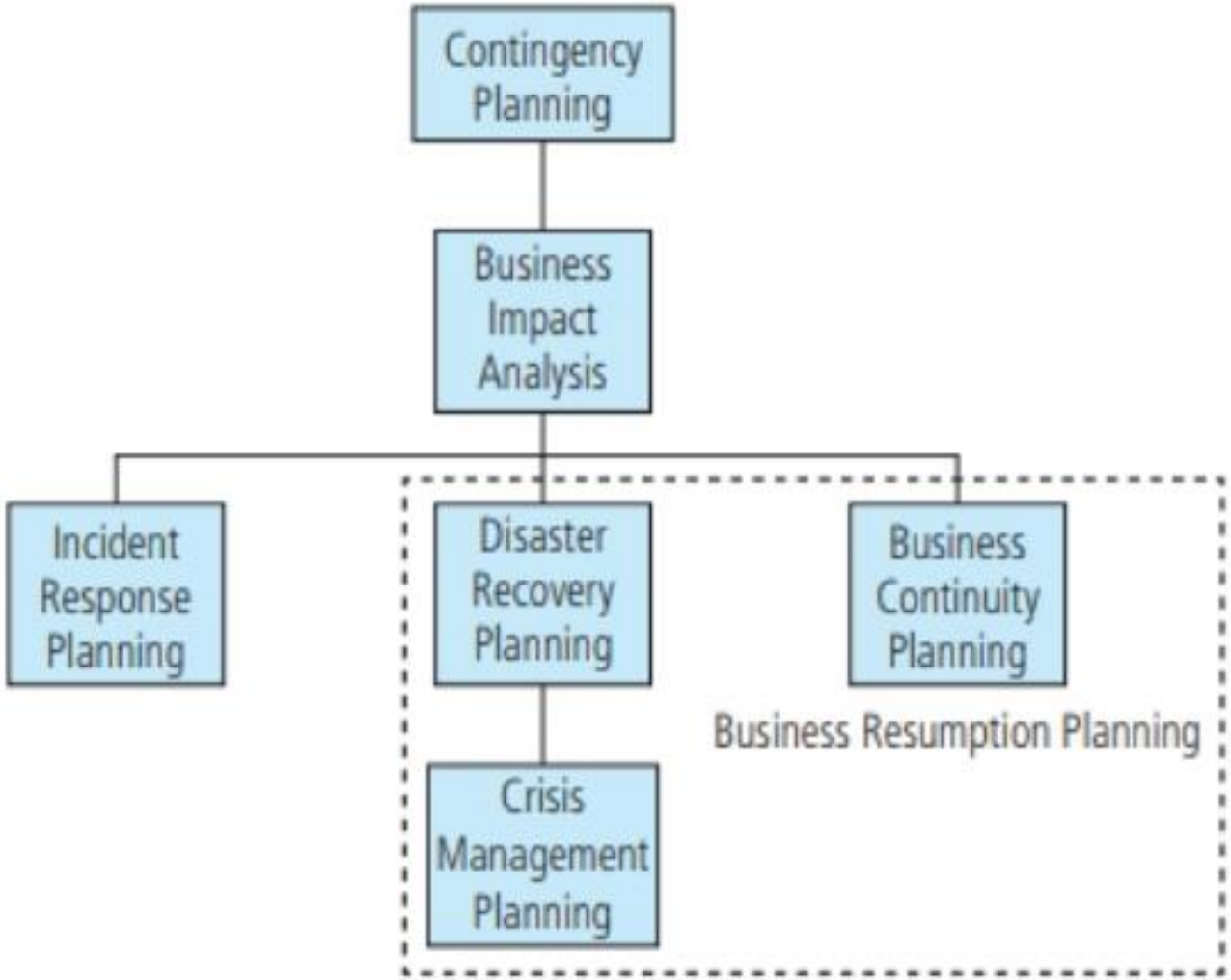
- Lập kế hoạch dự phòng (Contingency planning - CP) là quá trình mà các cộng đồng quan tâm đến CNTT và ATTT định vị tổ chức của họ để chuẩn bị, phát hiện, phản ứng và phục hồi từ các sự kiện đe dọa đến AT của tài nguyên và tài sản TT, cả con người và nhân tạo.
- Việc phát triển một kế hoạch để xử lý các sự kiện bất ngờ không mong muốn nên được ưu tiên hàng đầu đối với tất cả các nhà quản lý
- Để một kế hoạch được tất cả các thành viên của tổ chức coi là hợp lệ, kế hoạch đó phải được chấp thuận và được hỗ trợ tích cực bởi cộng đồng doanh nghiệp cùng quan tâm.

Kế hoạch dự phòng…

- CP được tạo thành từ bốn thành phần chính:
  - Quy trình thu thập dữ liệu và tài liệu được gọi là phân tích tác động kinh doanh (Business impact analysis - BIA)
  - Kế hoạch Ứng phó Sự cố (Incident response plan- IRP)
  - Kế hoạch khôi phục sau thảm họa (Disaster recovery plan - DRP)
  - Kế hoạch liên tục kinh doanh (Business continuity plan - BCP),
- Các tổ chức lớn có thể có nhiều loại kế hoạch và các tổ chức nhỏ có thể có một kế hoạch đơn giản, nhưng hầu hết đều có kế hoạch không đầy đủ
- có thể tạo và phát triển ba yếu tố lập kế hoạch của quá trình CP (kế hoạch IR, DR và BC) như một kế hoạch thống nhất hoặc có thể tạo ba yếu tố riêng biệt kết hợp với một tập hợp các thủ tục lồng ghép với nhau để cho phép tính liên tục.

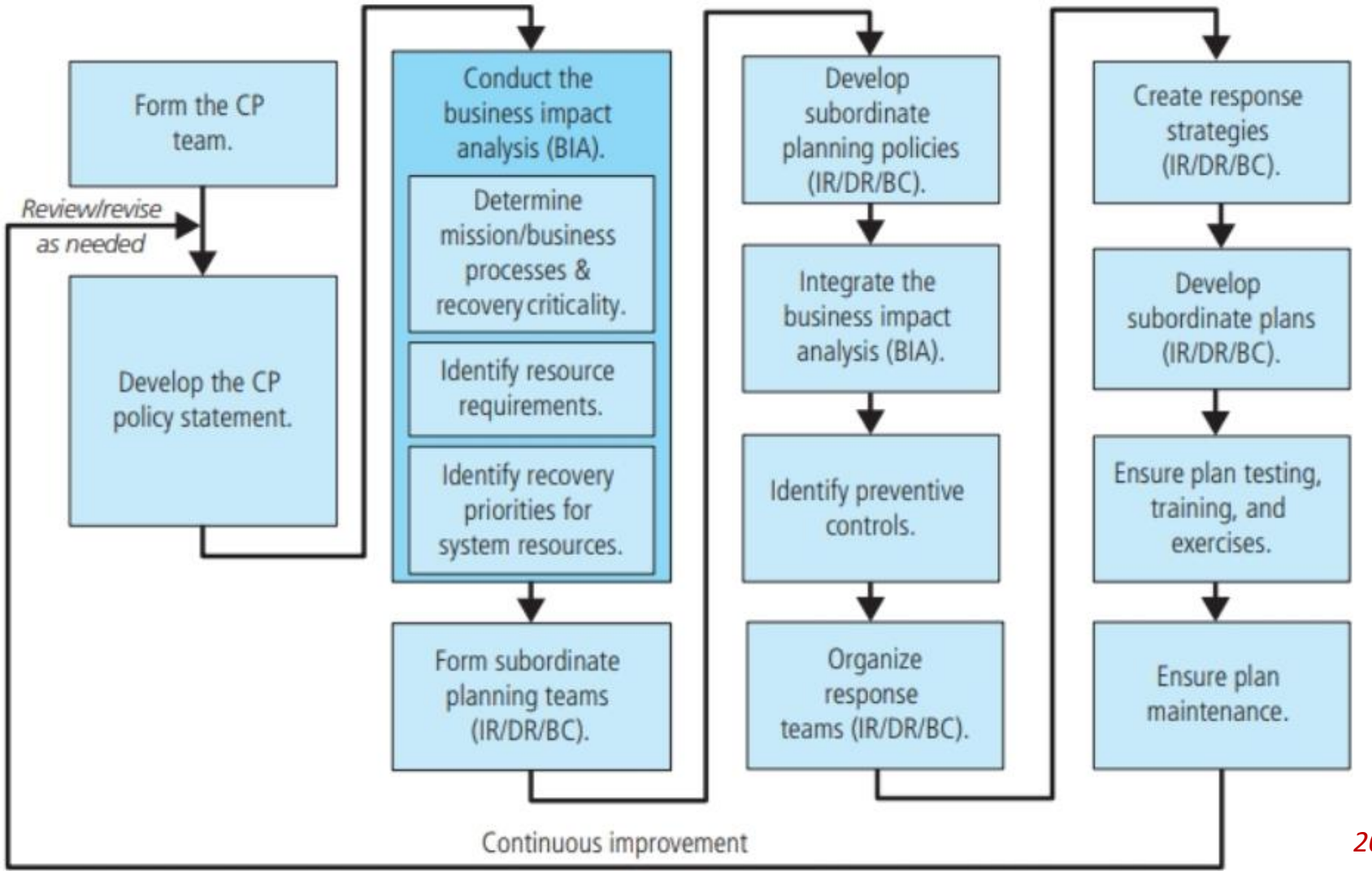
Kế hoạch dự phòng…

- Các thành phần: phân cấp lập kế hoạch dự phòng



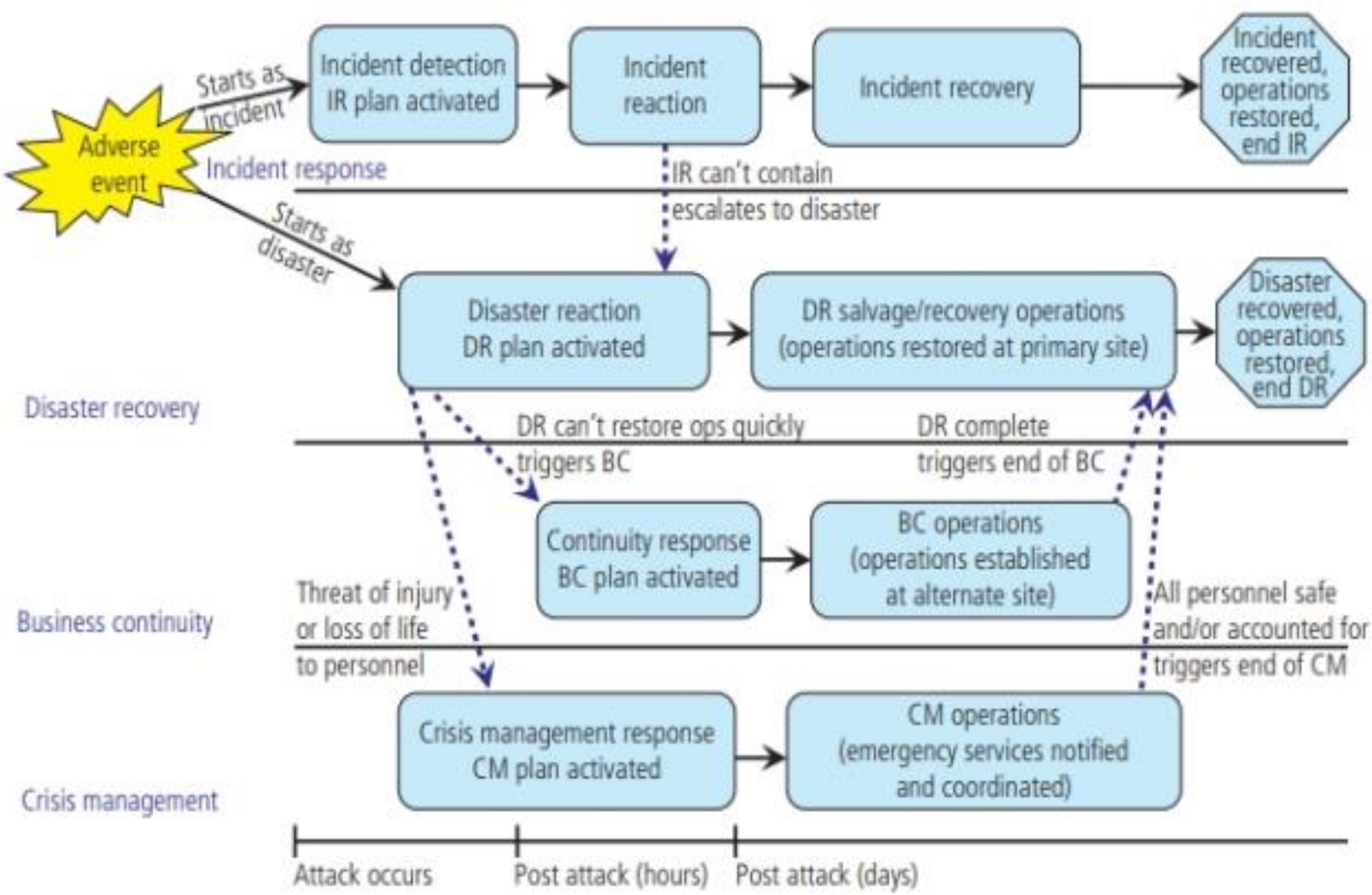
Kế hoạch dự phòng…

- Vòng đời kế hoạch dự phòng



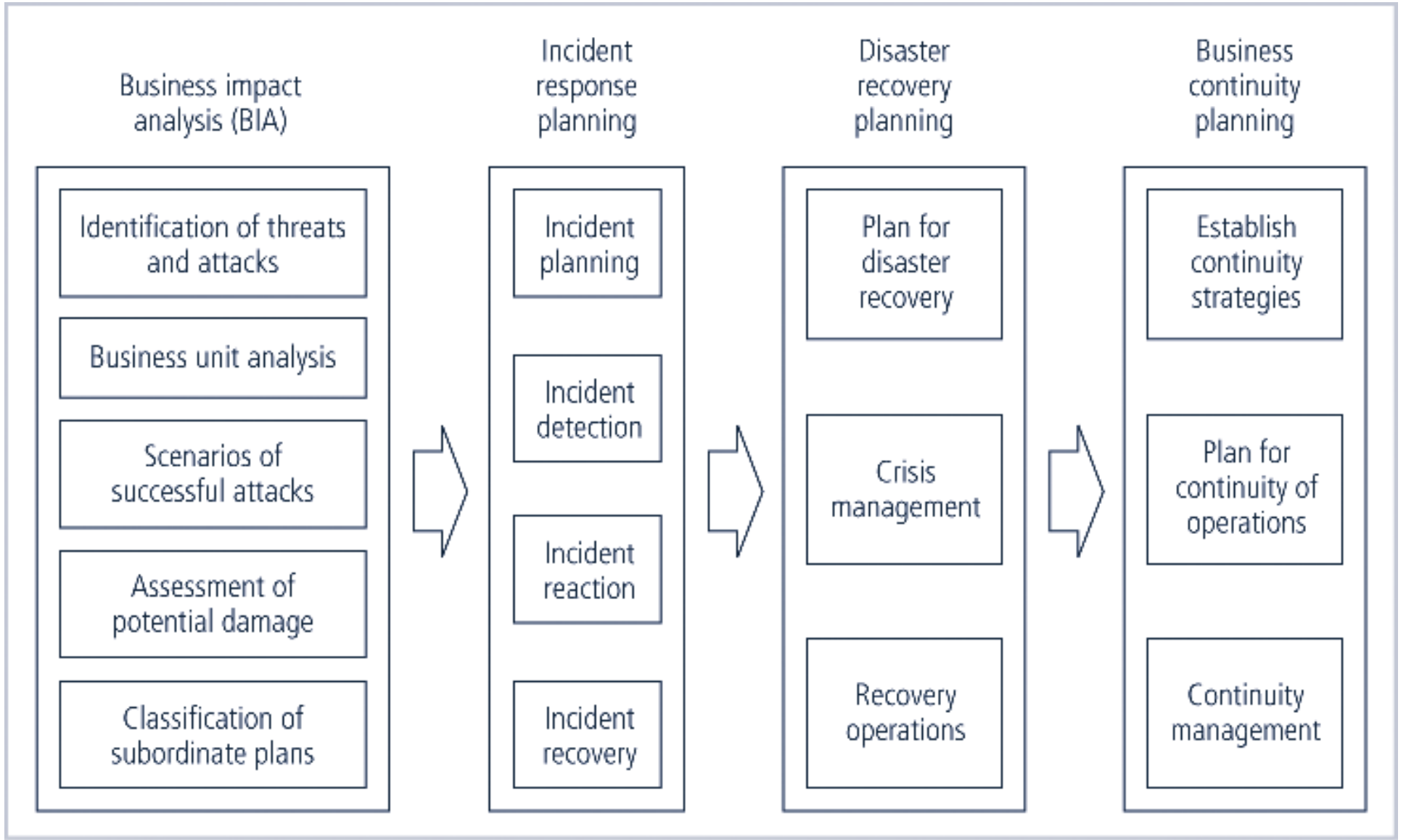
Kế hoạch dự phòng…

- Mốc thời gian của CP



Kế hoạch dự phòng…

- Các bước chính trong lập kế hoạch dự phòng



Kế hoạch dự phòng…

- Bốn nhóm tham gia vào việc lập kế hoạch dự phòng và các hoạt động dự phòng:
  - nhóm quản lý CP
  - nhóm IRP
  - nhóm DRP
  - nhóm BCP.

Kế hoạch dự phòng…

- Để đảm bảo tính liên tục trong quá trình tạo ra các thành phần CP, quy trình CP gồm 07 bước:
  1. Xây dựng tuyên bố chính sách lập kế hoạch dự phòng.
  2. Tiến hành BIA.
  3. Xác định các biện pháp kiểm soát phòng ngừa.
  4. Tạo chiến lược dự phòng
  5. Xây dựng kế hoạch dự phòng
  6. Đảm bảo kế hoạch kiểm tra, đào tạo và bài tập
  7. Đảm bảo duy trì kế hoạch.

Kế hoạch dự phòng…

- Chính sách lập kế hoạch dự phòng…
  - cho phép quá trình BIA và phải cung cấp hướng dẫn chính sách cụ thể về việc cho phép tạo ra từng thành phần lập kế hoạch (IR, DR và BC)
  - cung cấp hướng dẫn về cấu trúc của các nhóm cấp dưới và triết lý của tổ chức, và hỗ trợ trong việc cấu trúc kế hoạch.
  - có cấu trúc tương tự như tất cả các chính sách khác được tổ chức sử dụng
  - CSCP tối thiểu gồm…:
    - Một tuyên bố mở đầu về quan điểm triết học của quản lý cấp cao về tầm quan trọng của CP đối với các hoạt động chiến lược, dài hạn của tổ chức
    - Một tuyên bố về phạm vi và mục đích của các hoạt động CP, quy định yêu cầu bao gồm tất cả các chức năng và hoạt động kinh doanh quan trọng…

Kế hoạch dự phòng…

- Chính sách lập kế hoạch dự phòng
  - CSCP tối thiểu gồm:
    - Yêu cầu CPMT đánh giá rủi ro và BIA định kỳ.
    - Mô tả các thành phần chính của CP sẽ được CPMT thiết kế.
    - Lời kêu gọi và hướng dẫn lựa chọn các tùy chọn khôi phục và chiến lược liên tục.
    - Yêu cầu kiểm tra các kế hoạch khác nhau một cách thường xuyên.
    - Xác định các quy định và tiêu chuẩn chính có ảnh hưởng đến việc lập CP và tổng quan ngắn gọn về mức độ phù hợp của chúng.
    - Xác định các cá nhân chính chịu trách nhiệm về hoạt động CP.
    - Kêu gọi các thành viên cá nhân của tổ chức, yêu cầu họ hỗ trợ và củng cố tầm quan trọng của họ như một phần của quy trình CP tổng thể.
    - TT hành chính bổ sung, bao gồm ngày phát hành của tài liệu, ngày sửa đổi và lịch trình xem xét và bảo trì định kỳ.

Kế hoạch dự phòng…

- Phân tích tác động kinh doanh…
  - Là nền tảng quan trọng cho các giai đoạn lập kế hoạch ban đầu
  - Là một cuộc điều tra và đánh giá các sự kiện bất lợi có thể ảnh hưởng đến tổ chức, bao gồm việc xác định mức độ quan trọng của HT hoặc bộ thông tin đối với các quá trình cốt lõi của tổ chức và các ưu tiên phục hồi của nó.
  - giả định rằng các biện pháp kiểm soát AT đã bị bỏ qua, không thành công hoặc tỏ ra không hiệu quả, rằng cuộc tấn công đã thành công và rằng nghịch cảnh đang được bảo vệ chống lại đã thành công.

Kế hoạch dự phòng…

- Phân tích tác động kinh doanh…
  - bắt đầu với danh sách ưu tiên các mối đe dọa và lỗ hổng được xác định trong quá trình quản lý rủi ro và nâng cao danh sách bằng cách bổ sung thông tin cần thiết để ứng phó với nghịch cảnh
  - Khi thực hiện BIA cần cân nhắc những điều sau:
    1. Phạm vi
    2. Lập kế hoạch
    3. Sự cân bằng
    4. Mục tiêu
    5. Theo dõi

Kế hoạch dự phòng

- Phân tích tác động kinh doanh
  - Các bước thực hiện BIA
    - 1. Xác định sứ mệnh/quy trình kinh doanh và mức độ quan trọng của việc phục hồi.
    - 2. Xác định các yêu cầu về nguồn lực.
    - 3. Xác định các ưu tiên phục hồi cho tài nguyên hệ thống.

XÂY DỰNG KẾ HOẠCH DỰ PHÒNG

- Kế hoạch dự phòng
- Ứng cứu sự cố
- Khắc phục thảm họa
- Tính liên tục nghiệp vụ
- Quản lý khủng hoảng
- Kiểm tra kế hoạch dự phòng
- Câu hỏi ôn tập

Ứng cứu sự cố …

- Ứng phó sự cố (IR) là quá trình ngăn chặn, điều tra nguyên nhân, khôi phục hệ thống nhằm giảm thiểu các mối đe dọa liên quan tới vấn đề ATTT.
- IRP là một tập hợp chi tiết các quy trình và thủ tục lập kế hoạch, phát hiện và giải quyết các ảnh hưởng của một sự kiện bất ngờ đối với tài nguyên và tài sản TT, hướng dẫn giúp người ứng phó sự cố phát hiện và ứng phó với các sự cố AT.
- Lập kế hoạch ứng phó sự cố ATTT là một bước quan trọng đầu tiên của quản lý sự cố ATTT. Lãnh đạo cao nhất phải xác nhận kế hoạch này và tham gia vào mọi bước của chu trình quản lý sự cố.
- IR là một biện pháp phản ứng, không phải là một biện pháp phòng ngừa, mặc dù hầu hết các kế hoạch IR đều bao gồm các khuyến nghị phòng ngừa.

Ứng cứu sự cố…

- Lợi ích…:
  - Chuẩn bị tốt trong trường hợp khẩn cấp — các sự cố AT xảy ra mà không có cảnh báo trước, vì vậy điều cần thiết là phải chuẩn bị trước một quy trình
  - Quy trình lặp lại — không có kế hoạch ứng phó sự cố, các nhóm không thể phản hồi theo cách lặp lại hoặc ưu tiên thời gian của họ
  - Phối hợp — trong các tổ chức lớn, khó có thể giữ mọi người ở trong cuộc khi xảy ra khủng hoảng. Quy trình ứng phó sự cố có thể giúp đạt được điều này
  - Để lộ những lỗ hổng — trong các tổ chức quy mô vừa với số lượng nhân viên hạn chế hoặc trình độ kỹ thuật hạn chế, một kế hoạch ứng phó sự cố bộc lộ những lỗ hổng rõ ràng trong quy trình AT hoặc công cụ có thể được giải quyết trước khi khủng hoảng xảy ra

Ứng cứu sự cố…

- Lợi ích:
  - Lưu giữ kiến thức quan trọng — một kế hoạch ứng phó sự cố đảm bảo kiến thức quan trọng và các phương pháp hay nhất để đối phó với khủng hoảng không bị lãng quên theo thời gian và các bài học kinh nghiệm được bổ sung từng bước
  - Làm cho việc thực thi hoàn hảo — một kế hoạch ứng phó sự cố tạo ra một quy trình rõ ràng, có thể lặp lại và được tuân theo trong mọi sự cố, cải thiện sự phối hợp và hiệu quả của ứng phó theo thời gian
  - Tài liệu và trách nhiệm giải trình — một kế hoạch ứng phó sự cố với tài liệu rõ ràng làm giảm trách nhiệm pháp lý của tổ chức — nó cho phép chứng minh với các kiểm toán viên hoặc cơ quan chức năng về việc tuân thủ những gì đã được thực hiện để ngăn chặn vi phạm.

Ứng cứu sự…

- Nguyên tắc:
  - Không có giải pháp đơn giản phù hợp với tất cả tổ chức có cùng kích cỡ
  - Cam kết của lãnh đạo cao nhất
  - Thu hút mọi thành viên trong tổ chức
  - Lưu một bản sao ngoại tuyến của các tài liệu cần khi có sự cố
  - Không liên kết các bản sao lưu với phần còn lại của hệ thống
  - Việc ghi nhật ký là rất quan trọng và lưu những nhật ký đó trong một thời gian nhất định (lên đến 6 tháng)
  - Luôn cập nhật kế hoạch ứng phó ATTT và tất cả các thông tin và tài liệu liên quan
  - Đảm bảo rằng có tính đến tất cả các khía cạnh pháp lý khi quản lý sự cố ATTT
  - Ghi lại từng bước của một sự cố ATTT.

Ứng cứu sự cố…

- Các yếu tố cần được đưa vào kế hoạch ứng phó sự cố ATTT:
  - Xác định các tài sản cần được bảo vệ;
  - Xác định và phân công trách nhiệm trong bối cảnh xảy ra sự cố ATTT;
  - Khả năng nội bộ hoặc hợp đồng với các chuyên gia bên ngoài để ứng phó sự cố và/hoặc điều tra pháp y trong trường hợp xảy ra sự cố ATTT thực sự;
  - Thiết bị và công nghệ phát hiện và xử lý sự cố ATTT;
  - Chiến lược ngăn chặn cơ bản: ngắt kết nối HT ngay lập tức để khôi phục càng nhanh càng tốt hay dành thời gian để thu thập bằng chứng chống lại tội phạm đã gây ra cho HT?
  - Một chiến lược truyền thông cho cả các bên liên quan bên trong và bên ngoài và cho các cơ quan chức năng như cơ quan thực thi pháp luật, ….
  - Các tổ chức nên xem xét việc mua bảo hiểm.

Ứng cứu sự cố…

❖ Quy trình ứng cứu sự cố

1. Bắt đầu
2. Chính sách ứng cứu sự cố
3. Lập kế hoạch ứng cứu sự cố
4. Phát hiện sự cố
5. Phản ứng sự cố
6. Phục hồi sau sự cố

Ứng cứu sự cố…

- 1. Bắt đầu:
  - CPMT hình thành IRPT, bắt đầu hoạt động bằng cách phát triển CS xác định hoạt động của nhóm, nêu rõ phản ứng của tổ chức đối với các loại sự cố khác nhau và tư vấn cho người dùng cách đóng góp vào phản ứng hiệu quả của tổ chức , thay vì góp phần vào vấn đề đang xảy ra.
  - IRPT hình thành nhóm ứng phó sự cố bảo mật máy tính (CSIRT)

Ứng cứu sự cố…

- 2. Chính sách ứng cứu sự cố…
  - Các thành phần chính của một chính sách IR điển hình:
    1. Tuyên bố cam kết quản lý
    2. Mục đích và mục tiêu của chính sách
    3. Phạm vi của chính sách
    4. Định nghĩa các sự cố InfoSec và các thuật ngữ liên quan
    5. Cơ cấu tổ chức và định nghĩa về vai trò, trách nhiệm và cấp độ quyền hạn
    6. Xếp hạng mức độ ưu tiên hoặc mức độ nghiêm trọng của các sự cố
    7. Các biện pháp thực hiện
    8. Báo cáo và biểu mẫu liên hệ

Ứng cứu sự cố…

- 2. Chính sách ứng cứu sự cố
  - phải được sự hỗ trợ đầy đủ của lãnh đạo cao nhất và được tất cả các bên bị ảnh hưởng hiểu rõ ràng

=> đảm bảo rằng CSIRT đang thực hiện các hành động được ủy quyền; bảo vệ cả các thành viên CSIRT và tổ chức khỏi sự hiểu lầm và trách nhiệm pháp lý tiềm ẩn.

Ứng cứu sự cố…

- 3. Lập kế hoạch ứng cứu sự cố…
  - Trách nhiệm tạo kế hoạch IR của tổ chức thường thuộc về CIO, CISO hoặc người quản lý CNTT có trách nhiệm về ATTT
  - CISO nên chọn các thành viên từ mỗi cộng đồng liên quan để thành lập một nhóm IR độc lập, nhóm này thực hiện kế hoạch IR.
  - Vai trò và trách nhiệm của các thành viên trong nhóm IR được lập thành văn bản và truyền đạt rõ ràng trong toàn tổ chức.
  - IRP cũng bao gồm một danh sách cảnh báo, liệt kê một số cá nhân và tổ chức quan trọng nhất định cần được liên hệ trong quá trình xảy ra sự cố.

Ứng cứu sự cố…

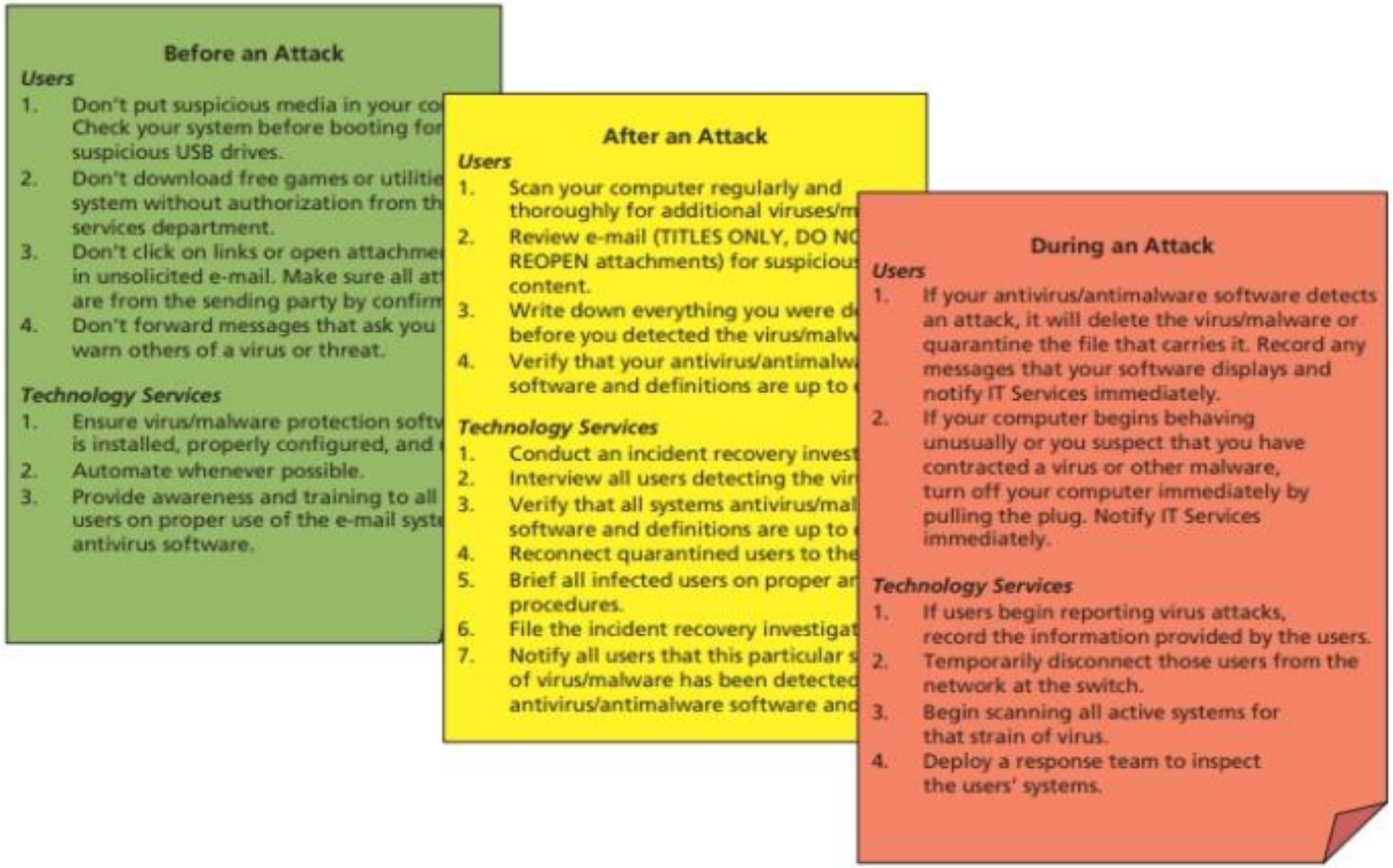
- 3. Lập kế hoạch ứng cứu sự cố…
  - IRP nên bao gồm các yếu tố sau:
    1. Sứ mệnh
    2. Chiến lược và mục tiêu
    3. Sự chấp thuận của quản lý cấp cao
    4. Cách tiếp cận của tổ chức để ứng cứu sự cố
    5. Cách nhóm ứng cứu sự cố sẽ giao tiếp với phần còn lại của tổ chức và với các tổ chức khác
    6. Các chỉ số đo lường khả năng ứng cứu sự cố và hiệu quả
    7. Lộ trình để hoàn thiện khả năng ứng cứu sự cố
    8. Chương trình phù hợp với tổ chức tổng thể như thế nào
  - Trong quá trình lập kế hoạch này, các quy trình IR thường được gọi là quy trình hoạt động tiêu chuẩn (SOP) sẽ hình thành

Ứng cứu sự cố…

- 3. Lập kế hoạch ứng cứu sự cố…
  - Đối với mọi tình huống sự cố, nhóm CP tạo ra ba bộ quy trình xử lý sự cố:
    1. Trong khi xảy ra sự cố.
    2. Sau khi sự cố xảy ra.
    3. Trước khi sự cố xảy ra

Ứng cứu sự cố…

- 3. Lập kế hoạch ứng cứu sự cố…
  - Ví dụ về các thủ tục xử lý sự cố IRP



Before an Attack

Users

1. Don't put suspicious media in your co… Check your system before booting for… suspicious USB drives.
2. Don't download free games or utilitie… system without authorization from th… services department.
3. Don't click on links or open attachme… in unsolicited e-mail. Make sure all at… are from the sending party by confirm…
4. Don't forward messages that ask you … warn others of a virus or threat.

Technology Services

1. Ensure virus/malware protection softv… is installed, properly configured, and …
2. Automate whenever possible.
3. Provide awareness and training to all … users on proper use of the e-mail syst… antivirus software.

After an Attack

Users

1. Scan your computer regularly and thoroughly for additional viruses/m…
2. Review e-mail (TITLES ONLY, DO NO… REOPEN attachments) for suspicious… content.
3. Write down everything you were d… before you detected the virus/malw…
4. Verify that your antivirus/antimalwa… software and definitions are up to …

Technology Services

1. Conduct an incident recovery invest…
2. Interview all users detecting the vir…
3. Verify that all systems antivirus/mal… software and definitions are up to …
4. Reconnect quarantined users to the…
5. Brief all infected users on proper ar… procedures.
6. File the incident recovery investigat…
7. Notify all users that this particular s… of virus/malware has been detected… antivirus/antimalware software and…

During an Attack

Users

1. If your antivirus/antimalware software detects an attack, it will delete the virus/malware or quarantine the file that carries it. Record any messages that your software displays and notify IT Services immediately.
2. If your computer begins behaving unusually or you suspect that you have contracted a virus or other malware, turn off your computer immediately by pulling the plug. Notify IT Services immediately.

Technology Services

1. If users begin reporting virus attacks, record the information provided by the users.
2. Temporarily disconnect those users from the network at the switch.
3. Begin scanning all active systems for that strain of virus.
4. Deploy a response team to inspect the users' systems.

Ứng cứu sự cố…

- 3. Lập kế hoạch ứng cứu sự cố…
  - Việc thực hiện kế hoạch IR thường thuộc về CSIRT
  - cách triển khai chính thức hơn, CSIRT là một tập hợp các chính sách, thủ tục, công nghệ, con người và dữ liệu được đưa ra để ngăn chặn, phát hiện, phản ứng và phục hồi từ một sự cố có thể làm hỏng thông tin của tổ chức
  - CSIRT phải sẵn sàng liên hệ với bất kỳ ai phát hiện ra hoặc nghi ngờ rằng một sự cố liên quan đến tổ chức đã xảy ra.
  - CSIRT bao gồm các chuyên gia có khả năng xử lý hệ thống thông tin và các khu vực chức năng bị ảnh hưởng bởi sự cố.

Ứng cứu sự cố…

- 3. Lập kế hoạch ứng cứu sự cố…
  - Các hành động ứng cứu sự cố có thể được tổ chức thành ba giai đoạn cơ bản:
    - Phát hiện- Nhận biết rằng một sự cố đang được tiến hành
    - Phản ứng- Phản ứng với sự cố theo cách thức định trước để ngăn chặn và giảm thiểu thiệt hại tiềm ẩn của nó
    - Phục hồi- Trả lại tất cả các hệ thống và dữ liệu về trạng thái của chúng trước khi xảy ra sự cố

Ứng cứu sự cố…

- 3. Lập kế hoạch ứng cứu sự cố…
  - Phát hiện và phân tích…
    1. Xác định xem một sự cố đã xảy ra
       1. Phân tích các tiền chất và chỉ số
       2. Tìm kiếm thông tin tương quan
       3. Thực hiện nghiên cứu (ví dụ: công cụ tìm kiếm, cơ sở kiến thức)
       4. Ngay khi người xử lý tin rằng một sự cố đã xảy ra, hãy bắt đầu lập hồ sơ điều tra và thu thập bằng chứng
    2. Ưu tiên xử lý sự cố dựa trên các yếu tố liên quan (tác động chức năng, tác động thông tin, nỗ lực khôi phục, v.v.)
    3. Báo cáo sự cố cho nhân viên nội bộ thích hợp và các tổ chức bên ngoài

Ứng cứu sự cố…

- 3. Lập kế hoạch ứng cứu sự cố…
  - Kiểm soát, xóa bỏ và phục hồi
    4. Thu thập, bảo quản, bảo mật và lập hồ sơ bằng chứng
    5. Chứa đựng sự cố
    6. Xóa bỏ sự cố
       1. Xác định và giảm thiểu tất cả các lỗ hổng đã bị khai thác
       2. Xóa phần mềm độc hại, tài liệu không phù hợp và các thành phần khác
       3. Nếu phát hiện nhiều máy chủ bị ảnh hưởng hơn (ví dụ: nhiễm phần mềm độc hại mới), hãy lặp lại các bước Phát hiện và Phân tích (1.1, 1.2) để xác định tất cả các máy chủ bị ảnh hưởng khác, sau đó chứa (5) và xóa (6) sự cố cho chúng
    7. Phục hồi sau sự cố
       1. Đưa các hệ thống bị ảnh hưởng về trạng thái sẵn sàng hoạt động
       2. Xác nhận rằng các hệ thống bị ảnh hưởng đang hoạt động bình thường
       3. Nếu cần, thực hiện giám sát bổ sung để tìm kiếm hoạt động liên quan trong tương lai

Ứng cứu sự cố…

- 3. Lập kế hoạch ứng cứu sự cố…
  - Hoạt động sau sự cố
    - 8. Tạo một báo cáo tiếp theo
    - 9. Tổ chức một cuộc họp rút kinh nghiệm (bắt buộc đối với các sự cố lớn, nếu không thì tùy chọn)

Ứng cứu sự cố…

- 3. Lập kế hoạch ứng cứu sự cố
  - Bảo vệ dữ liệu trong quá trình chuẩn bị cho sự cố
    - Các tuỳ chọn
      - Sao lưu dữ liệu truyền thống
      - Kho lưu trữ điện tử
      - Ghi nhật ký từ xa
      - CSDL shadowing
    - Khuyến nghị:
      - quy tắc “3-2-1“
      - các bản sao lưu hàng ngày được lưu trữ tại chỗ và bản sao lưu hàng tuần được lưu trữ bên ngoài.

Ứng cứu sự cố…

- 4. Phát hiện sự cố…
  - Phân loại sự cố là quá trình mà nhóm IR xem xét một ứng cử viên sự cố và xác định xem nó có cấu thành một sự cố thực sự hay không.
  - Sau khi sự cố thực tế được xác định và phân loại đúng, các thành viên của nhóm IR có thể thực hiện hiệu quả các thủ tục tương ứng từ IRP.
  - Ba loại chỉ số sự cố được sử dụng: có thể, có thể xảy ra và xác định

Ứng cứu sự cố…

- 4. Phát hiện sự cố…
  - Chỉ số có thể:
    - Sự hiện diện của các tệp không quen thuộc
    - Hiện diện hoặc thực thi các chương trình hoặc quy trình không xác định
    - Tiêu thụ tài nguyên máy tính một cách bất thường
    - Hệ thống bị treo bất thường

Ứng cứu sự cố…

- 4. Phát hiện sự cố…
  - Chỉ số có thể xảy ra
    - Hoạt động vào những thời điểm không mong muốn
    - Sự hiện diện của các tài khoản mới
    - Các cuộc tấn công được báo cáo
    - Thông báo từ IDPS

Ứng cứu sự cố…

- 4. Phát hiện sự cố…
  - Chỉ số xác định
    - Sử dụng tài khoản không bình thường
    - Thay đổi nhật ký
    - Sự hiện diện của các công cụ của hacker
    - Thông báo của đối tác hoặc đồng nghiệp
    - Thông báo của tin tặc

Ứng cứu sự cố…

- 4. Phát hiện sự cố…
  - Kết quả của sự cố tiềm ẩn
    - Mất tính khả dụng
    - Mất tính toàn vẹn
    - Mất tính bảo mật
    - Vi phạm chính sách
    - Vi phạm pháp luật hoặc quy định.

Ứng cứu sự cố…

- 5. Phản ứng sự cố
  - Thông báo của Nhân sự Chủ chốt: Có hai cách để kích hoạt danh sách cảnh báo: tuần tự và phân cấp (có sẵn nhiều HT tự động tạo điều kiện thuận lợi cho cả hai cách tiếp cận)
  - Ghi lại sự cố: phải ghi lại ai, cái gì, khi nào, ở đâu, tại sao và cách thức của từng hành động được thực hiện trong khi sự cố đang xảy ra.
  - Các chiến lược ngăn chặn sự cố:
    - Vô hiệu hóa tài khoản người dùng bị xâm phạm
    - Cấu hình lại tường lửa để chặn lưu lượng sự cố
    - Tạm thời vô hiệu hóa quy trình hoặc dịch vụ bị xâm phạm
    - Gỡ bỏ ứng dụng ống dẫn hoặc máy chủ - ví dụ: máy chủ e-mail
    - Ngắt kết nối mạng hoặc phân đoạn mạng bị ảnh hưởng
    - Dừng (tắt nguồn) tất cả các máy tính và thiết bị mạng
  - Báo cáo sự cố: trong quá trình BIA, phải xác định thời điểm một sự cố được coi là một thảm họa. Các tiêu chí này phải được bao gồm trong IRP. Tổ chức cũng phải lập thành văn bản khi nào cần sự tham gia của những người phản ứng bên ngoài

Ứng cứu sự cố…

- 6. Phục hồi sau sự cố…
  - Khi sự cố đã được kiểm soát và kiểm soát hệ thống đã được khôi phục, quá trình khắc phục sự cố có thể bắt đầu.
  - thông báo cho nguồn nhân lực phù hợp
  - CSIRT phải đánh giá toàn bộ mức độ thiệt hại để xác định những gì phải làm để khôi phục hệ thống
    - xác định ngay phạm vi vi phạm về tính bí mật, tính toàn vẹn và tính sẵn sàng của TT và tài sản TT được gọi là đánh giá thiệt hại do sự cố
    - Khi mức độ thiệt hại đã được xác định, quá trình khôi phục bắt đầu.

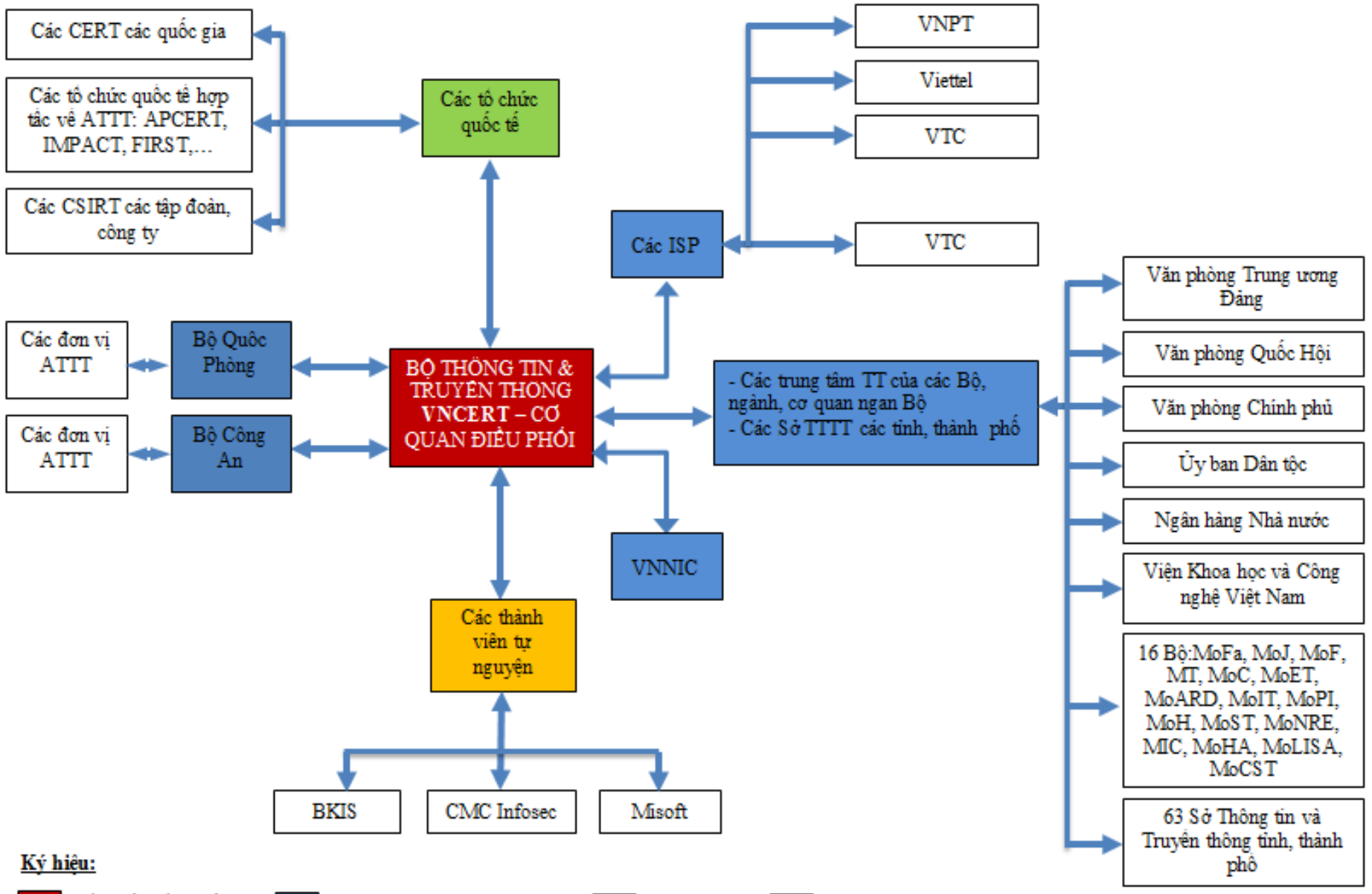
Ứng cứu sự cố…

- 6. Phục hồi sau sự cố…
  - Quá trình khôi phục:
    - Xác định các lỗ hổng cho phép sự cố xảy ra và lan rộng. Giải quyết chúng.
    - Xử lý các biện pháp bảo vệ không thể ngăn chặn hoặc hạn chế sự cố hoặc không có trong HT ngay từ đầu. Cài đặt, thay thế hoặc nâng cấp chúng.
    - Đánh giá khả năng giám sát (nếu có). Cải thiện các phương pháp phát hiện và báo cáo hoặc cài đặt các khả năng giám sát mới.
    - 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 niềm tin của các thành viên trong cộng đồng quan tâm của tổ chức => để ngăn chặn sự hoảng loạn hoặc nhầm lẫn gây ra gián đoạn thêm cho hoạt động của tổ chức.

Ứng cứu sự cố…

- 6. Phục hồi sau sự cố…
  - Triết lý tổ chức về xử lý sự cố và thảm họa: phải chọn một trong hai triết lý sẽ ảnh hưởng đến cách tiếp cận IR và DR cũng như sự tham gia sau đó của pháp y kỹ thuật số và thực thi pháp luật:
    - Bảo vệ và quên- còn gọi là "vá và tiếp tục" tập trung vào việc bảo vệ dữ liệu và HT lưu trữ, sử dụng và truyền tải dữ liệu đó.
    - Bắt giữ và truy tố- còn gọi là "đuổi bắt và truy tố" tập trung vào việc xác định và bắt giữ các cá nhân có trách nhiệm, trong đó chú ý hơn đến việc thu thập và bảo quản tài liệu chứng minh tiềm năng có thể hỗ trợ việc truy tố hành chính hoặc hình sự.

Mạng lưới ứng cứu sự cố ATTT quốc gia



Sự cố và thảm hoạ…

- Khi nào sự cố trở thành thảm họa?
  - Tổ chức không thể giảm thiểu tác động của một sự cố trong khi sự cố xảy ra
  - Mức độ thiệt hại hoặc phá hủy quá nghiêm trọng khiến tổ chức không thể nhanh chóng phục hồi
- Sự khác biệt có thể là tinh tế
- Tùy thuộc vào tổ chức để quyết định sự cố nào được phân loại là thảm họa và do đó nhận được mức độ phản ứng thích hợp

Sự cố và thảm hoạ

Incident: Ransomware attack on a single system/user

Disaster: Ransomware attack on all organizational systems/users

Attack occurs: Depending on scope, may be classified as an incident or a disaster

XÂY DỰNG KẾ HOẠCH DỰ PHÒNG

- Kế hoạch dự phòng
- Ứng cứu sự cố
- **Khắc phục thảm họa**
- Tính liên tục nghiệp vụ
- Quản lý khủng hoảng
- Kiểm tra kế hoạch dự phòng
- Câu hỏi ôn tập

Khắc phục thảm hoạ…

- Lập kế hoạch phục hồi sau thảm họa (DRP) đòi hỏi sự chuẩn bị và phục hồi sau thảm họa, cho dù là tự nhiên hay nhân tạo.
- Thảm hoạ:
  - Những sự cố mà IRP có thể không còn khả năng xử lý và khôi phục hiệu quả tổn thất.
  - Các sự kiện về bản chất ngay lập tức được phân loại là thảm họa, chẳng hạn như hỏa hoạn trên diện rộng, lũ lụt, bão gây thiệt hại hoặc động đất

Khắc phục thảm hoạ…

- nhóm CP tạo ra nhóm lập kế hoạch DR (DRPT). DRPT lần lượt tổ chức và chuẩn bị cho các đội ứng phó DR (DRRT) để thực hiện DRP trong trường hợp có thiên tai. Trong thực tế, có thể có nhiều DRRT khác nhau, mỗi DRRT có nhiệm vụ phục hồi một khía cạnh khác nhau.
- Một số DRRT phổ biến bao gồm:
  - Nhóm quản lý DR.
  - Nhóm truyền thông
  - Nhóm khôi phục máy tính (phần cứng)
  - Nhóm khôi phục hệ thống (OS)
  - Nhóm khôi phục mạng
  - Nhóm khôi phục lưu trữ
  - Nhóm khôi phục ứng dụng
  - Nhóm quản lý dữ liệu
  - Nhóm liên hệ với nhà cung cấp
  - Đội đánh giá thiệt hại và cứu hộ
  - Nhóm giao diện kinh doanh
  - Nhóm hậu cần
  - Các đội khác nếu cần.

Khắc phục thảm hoạ…

- Nhiệm vụ của các nhóm:
  - Khôi phục các tài sản TT có thể tận dụng được từ cơ sở chính sau thảm họa.
  - Mua hoặc thay thế các tài sản thông tin đã được mua từ các nguồn thích hợp.
  - Thiết lập lại các tài sản thông tin chức năng tại địa điểm chính nếu có thể hoặc tại địa điểm chính mới, nếu cần.

Khắc phục thảm hoạ…

- Quy trình DRP:
  1. Quá trình khắc phục thảm họa
  2. Chính sách khắc phục thảm họa
  3. Phân loại thảm họa
  4. Lập kế hoạch phục hồi
  5. Ứng phó với thảm họa
  6. Kế hoạch khắc phục thảm họa đơn giản

Khắc phục thảm hoạ…

- 1. Quá trình khắc phục thảm họa…
  - một thảm họa đã xảy ra khi một trong hai tiêu chí được đáp ứng:
    - Tổ chức không thể ngăn chặn hoặc kiểm soát tác động của một sự cố
    - mức độ thiệt hại hoặc tàn phá của một sự cố quá nghiêm trọng đến mức tổ chức không thể nhanh chóng phục hồi từ nó.
  - Vai trò quan trọng của kế hoạch DR là chuẩn bị để thiết lập lại hoạt động tại địa điểm chính của tổ chức sau thảm họa hoặc thiết lập hoạt động tại địa điểm mới nếu địa điểm chính không còn khả thi.

Khắc phục thảm hoạ…

- 1. Quá trình khắc phục thảm họa
  - Quy trình DRP:
    1. Tổ chức nhóm DR
    2. Xây dựng tuyên bố chính sách lập kế hoạch DR
    3. Rà soát BIA
    4. Xác định các biện pháp kiểm soát phòng ngừa
    5. Tạo chiến lược DR
    6. Xây dựng tài liệu kế hoạch DR
    7. Đảm bảo kiểm tra, đào tạo và thực hành kế hoạch DR
    8. Đảm bảo duy trì kế hoạch DR.

Khắc phục thảm hoạ…

- 2. Chính sách khắc phục thảm họa…
  - trình bày tổng quan về triết lý của tổ chức về việc tiến hành các hoạt động DR và đóng vai trò là hướng dẫn cho việc phát triển DRP, có thể do nhóm CP của tổ chức tạo ra và được chuyển giao cho trưởng nhóm DR hoặc nhóm DR có thể được giao vai trò phát triển chính sách DR.

Khắc phục thảm hoạ…

- 2. Chính sách khắc phục thảm họa
  - chính sách DR chứa các yếu tố chính:
    1. Mục đích
    2. Phạm vi
    3. Vai trò và trách nhiệm
    4. Yêu cầu về nguồn lực
    5. Yêu cầu đào tạo.
    6. Lịch trình thực hiện và kiểm tra
    7. Lập kế hoạch lịch trình bảo trì
    8. Cân nhắc đặc biệt

Khắc phục thảm hoạ…

- 3. Phân loại thảm họa…
  - Phương pháp phân loại:
    - phổ biến nhất là đánh giá số lượng thiệt hại có thể gây ra bởi thiên tai - thường theo thang điểm Trung bình, Nghiêm trọng hoặc Đặc biệt nghiêm trọng.
    - theo nguồn gốc của chúng, chẳng hạn như tự nhiên hoặc nhân tạo.
    - theo tỷ lệ xuất hiện: thảm họa khởi phát chậm, thảm họa xảy ra nhanh.

Khắc phục thảm hoạ…

- 3. Phân loại thảm họa…
  - Cách giảm thiểu một số thảm hoạ tự nhiên:
    - Cháy: bảo hiểm tai nạn hỏa hoạn hoặc bảo hiểm gián đoạn kinh doanh
    - Lũ lụt: bảo hiểm lũ lụt hoặc bảo hiểm gián đoạn kinh doanh
    - Động đất: bảo hiểm thương vong cụ thể hoặc bảo hiểm gián đoạn kinh doanh, nhưng thường là một chính sách cụ thể và riêng biệt
    - Sét: bảo hiểm thương vong đa năng hoặc bảo hiểm gián đoạn kinh doanh.
    - Sạt lở đất: bảo hiểm thương vong hoặc bảo hiểm gián đoạn kinh doanh.
    - Lốc xoáy hoặc gió giật mạnh: bảo hiểm thương vong hoặc bảo hiểm gián đoạn kinh doanh
    - Bão: bảo hiểm thương vong hoặc bảo hiểm gián đoạn kinh doanh
    - Sóng thần: bảo hiểm thương vong hoặc bảo hiểm gián đoạn kinh doanh
    - Phóng tĩnh điện (ESD): bằng thiết bị phóng tĩnh điện đặc biệt và bằng cách quản lý mức nhiệt độ và độ ẩm HVAC
    - Ô nhiễm bụi: hệ thống lọc HVAC hiệu quả và các thủ tục đơn giản, chẳng hạn như quản lý nhà cửa hiệu quả, đặt thảm trải sàn dính ở lối vào và cấm sử dụng giấy và bìa cứng trong trung tâm dữ liệu.

Khắc phục thảm hoạ…

- 4. Lập kế hoạch phục hồi…
  - CPMT tham gia vào việc phát triển kịch bản và phân tích tác động, đồng thời phân loại mức độ đe dọa mà mỗi thảm họa tiềm ẩn gây ra.
  - Khi tạo một kịch bản DR, hãy bắt đầu với tài sản quan trọng nhất: con người
  - phải đào tạo chéo cho nhân viên của mình để đảm bảo rằng các hoạt động và tâm lý bình thường có thể được khôi phục
  - phải được kiểm tra thường xuyên để nhóm DR có thể đi đầu nỗ lực khôi phục một cách nhanh chóng và hiệu quả

Khắc phục thảm hoạ…

- 4. Lập kế hoạch phục hồi…
  - mỗi nhân viên phải luôn có hai loại thẻ thông tin khẩn cấp bên mình:
    - Liệt kê thông tin khẩn cấp cá nhân - người cần thông báo trong trường hợp khẩn cấp (người thân), tình trạng y tế và một hình thức nhận dạng.
    - chứa một tập hợp các hướng dẫn về những việc cần làm trong trường hợp khẩn cấp, phải chứa số liên lạc hoặc đường dây nóng để gọi cho tổ chức trong trường hợp khẩn cấp, số dịch vụ khẩn cấp (cứu hỏa, cảnh sát, y tế), địa điểm sơ tán và tập kết (ví dụ: khu trú bão), tên và số của Điều phối viên DR, và bất kỳ thông tin cần thiết nào khác.

Khắc phục thảm hoạ…

- 4. Lập kế hoạch phục hồi
  - Các yếu tố chính
    1. Phân quyền rõ ràng về vai trò và trách nhiệm
    2. Thực hiện danh sách cảnh báo và thông báo cho các nhân viên chủ chốt
    3. Xác lập quyền lợi rõ ràng
    4. Thủ tục lập hồ sơ về thảm họa
    5. Các bước hành động để giảm thiểu tác động của thảm họa đối với hoạt động của tổ chức
    6. Triển khai thay thế cho các thành phần HT khác nhau, nếu không có phiên bản chính

Khắc phục thảm hoạ…

- 5. Ứng phó với thảm họa
  - CPMT nên kết hợp mức độ linh hoạt vào kế hoạch
  - Nếu cơ sở vật chất còn nguyên vẹn, nhóm DR nên bắt đầu khôi phục hệ thống và dữ liệu để hướng tới khả năng hoạt động đầy đủ
  - Nếu cơ sở vật chất của tổ chức bị phá hủy, các hành động thay thế phải được thực hiện cho đến khi có được cơ sở vật chất mới. Khi một thảm họa đe dọa khả năng tồn tại của một tổ chức tại địa điểm chính, quy trình DR trở thành quy trình liên tục trong kinh doanh.

Khắc phục thảm hoạ…

- 6. Kế hoạch khắc phục thảm họa đơn giản…

1. Tên công ty
2. Ngày hoàn thành hoặc cập nhật kế hoạch.
3. Nhân viên sẽ được gọi trong trường hợp có thảm hoạ
4. Các dịch vụ khẩn cấp sẽ được gọi (nếu cần) trong trường hợp xảy ra thảm họa
5. Vị trí của thiết bị và vật tư khẩn cấp trong nhà
6. Nguồn cung cấp thiết bị và vật tư bên ngoài công trường
7. Danh sách ưu tiên cứu hộ
8. Các quy trình khắc phục hậu quả
9. Đánh giá tiếp theo

Khắc phục thảm hoạ…

- 6. Kế hoạch khắc phục thảm họa đơn giản

Disaster Recovery Plan Outline

1. Name of Company_____
2. Date of completion or update of the plan_____
3. Staff to be called in the event of a disaster:
   Name: Numbers: Position:
   …
   Note below who is to call whom upon the discovery of a disaster (Telephone Tree):
   …
4. Emergency services to be called (if needed) in event of a disaster:
   Service: Contact Person: Number:
   …
5. Locations of in-house emergency equipment and supplies (attach map or floor plan with locations marked):
   …
6. Sources of off-site equipment and supplies (if maintained on-site, note location):
   Item: Contact/Company: Number:
   …
7. Salvage Priority List:
   Attach a copy of the records retention schedule identifying all vital/essential records series. The location and record medium of the preservation duplicate for each vital records series should be noted.

   It is also very helpful if other records series are reviewed to determine their priority for salvage should a disaster occur. The following questions can be helpful in determining priorities:

   1) Can the records be replaced? At what cost?
   2) Would the cost of replacement be less or more than restoration of the records?
   3) How important are the records to the organization?
   4) Are the records duplicated elsewhere?

   To simplify this process, priorities may be assigned as follows:

   1) Salvage at all costs.
      (for example, records that are historically valuable or non-vital records that are important to operations and very difficult to recreate)
   2) Salvage if time and resources permit.
      (for example, records that are less important to the agency or somewhat easier to re-create)
   3) Dispose of as part of general cleanup.
      (for example, records that do not need to be salvaged because they are convenience copies and the record copy is at another location)
8. Disaster Recovery Procedures:
   Attach a list of specific procedures to be followed in the event of a disaster in your organization, including responsibilities of in-house recovery team members.
9. Follow-up Assessment:
   A written report, including photographs, should be prepared after recovery and attached to a copy of the disaster plan. The report should note the effectiveness of the plan, and should include an evaluation of the sources of supplies and equipment, and of any off-site facilities used.

XÂY DỰNG KẾ HOẠCH DỰ PHÒNG

- Kế hoạch dự phòng
- Ứng cứu sự cố
- Khắc phục thảm họa
- **Tính liên tục nghiệp vụ**
- Quản lý khủng hoảng
- Kiểm tra kế hoạch dự phòng
- Câu hỏi ôn tập

Tính liên tục nghiệp vụ…

- Tính liên tục nghiệp vụ (BC) - nỗ lực để đảm bảo khả năng tồn tại lâu dài của tổ chức khi một thảm họa ngăn cản hoạt động bình thường tại địa điểm chính. Tổ chức tạm thời thiết lập hoạt động quan trọng tại một địa điểm thay thế cho đến khi có thể tiếp tục hoạt động tại địa điểm chính hoặc chọn và chiếm lĩnh một địa điểm chính mới.
- Lập BCP đảm bảo các chức năng kinh doanh quan trọng vẫn tiếp tục nếu một sự cố nghiêm trọng hoặc thảm họa xảy ra. BCP có thể bao gồm các điều khoản cho địa điểm nóng, địa điểm ấm, địa điểm lạnh, chia sẻ thời gian, văn phòng dịch vụ và các thỏa thuận chung.
- Bởi DRP và BCP có liên quan chặt chẽ với nhau => chuẩn bị cả hai cùng một lúc và có thể kết hợp chúng thành một tài liệu kế hoạch duy nhất được gọi là KH tái hoạt động kinh doanh (BR).

Tính liên tục nghiệp vụ…

- DRP và BCP

Organizational disaster occurs

Staff implements DR/BC plans;
BC plan relocates organization to…

Alternate site

DR plan works to reestablish operations at

Primary site (or new permanent site)

Tính liên tục nghiệp vụ…

- Quy trình BCP:
  1. Hình thành nhóm BC
  2. Xây dựng tuyên bố chính sách lập kế hoạch BC
  3. Xem xét BIA
  4. Xác định các biện pháp kiểm soát phòng ngừa
  5. Tạo chiến lược tái định cư
  6. Xây dựng kế hoạch BC
  7. Đảm bảo kiểm tra, đào tạo và thực hành kế hoạch BC
  8. Đảm bảo duy trì kế hoạch BC

Tính liên tục nghiệp vụ…

- 2. Chính sách BC: bao gồm các phần chính sau:
  1. Mục đích
  2. Phạm vi
  3. Vai trò và trách nhiệm
  4. Yêu cầu về nguồn lực
  5. Yêu cầu đào tạo
  6. Lịch trình luyện tập và kiểm tra
  7. Lập kế hoạch lịch trình bảo trì
  8. Cân nhắc đặc biệt.

Tính liên tục nghiệp vụ…

- 5. Chiến lược BC
  - Chiến lược độc quyền:
    - Địa điểm nóng
    - Địa điểm ấm
    - Địa điểm lạnh
  - Chiến lược chia sẻ:
    - Chia sẻ thời gian
    - Văn phòng dịch vụ
    - Thoả thuận lẫn nhau
  - các lựa chọn thay thế chuyên biệt
    - Địa điểm di động lăn bánh, được định cấu hình trong khu vực trọng tải của máy kéo/rơ moóc
    - các tài nguyên được lưu trữ bên ngoài, như khu vực lưu trữ cho thuê chứa thiết bị trùng lặp hoặc cũ hơn.

XÂY DỰNG KẾ HOẠCH DỰ PHÒNG

- Kế hoạch dự phòng
- Ứng cứu sự cố
- Khắc phục thảm họa
- Tính liên tục nghiệp vụ
- **Quản lý khủng hoảng**
- Kiểm tra kế hoạch dự phòng
- Câu hỏi ôn tập

Quản lý khủng hoảng…

- Quản lý khủng hoảng (CM - Crisis Management) - Một tập hợp các nỗ lực lập kế hoạch và chuẩn bị của một tổ chức để đối phó với thương tích tiềm ẩn ở người, chấn thương tinh thần hoặc mất mạng do thảm họa.
- Cách thức thiết lập
  - Thuộc DRP
  - CMP riêng
- DRRT làm việc chặt chẽ với CMRT để đảm bảo thông tin liên lạc đầy đủ và kịp thời trong thời gian xảy ra thảm hoạ.

Quản lý khủng hoảng…

- vai trò của CMPT:
  1. Hỗ trợ nhân sự và những người thân yêu của họ trong thời kỳ khủng hoảng
  2. Thông báo cho công chúng về sự kiện và các hành động được thực hiện để đảm bảo sự phục hồi của nhân sự và doanh nghiệp
  3. Giao tiếp với các khách hàng lớn, nhà cung cấp, đối tác, cơ quan quản lý, tổ chức trong ngành, giới truyền thông và các bên liên quan khác

Quản lý khủng hoảng…

- Trách nhiệm của CMPT:
  1. Xác minh tình trạng nhân sự
  2. Kích hoạt danh sách cảnh báo
  3. Phối hợp với các dịch vụ khẩn cấp
- CMPT nên lập kế hoạch một cách tiếp cận để công bố thông tin trong trường hợp xảy ra thảm họa và thậm chí nên có các kịch bản soạn sẵn chuẩn bị cho các thông cáo báo chí.

Quản lý khủng hoảng

- CM được tổ chức và tiến hành như một thực thể riêng biệt, thì CM đó phải có chính sách CM và kế hoạch CM
- Các phương pháp luận có thể tuân theo các mô hình cơ bản tương tự DR, nhưng phải bao gồm các nội dung bổ sung tập trung vào an toàn nhân sự (chẳng hạn như khu vực trú ẩn), kế hoạch sơ tán, thông tin liên hệ cho các dịch vụ khẩn cấp, …

XÂY DỰNG KẾ HOẠCH DỰ PHÒNG

- Kế hoạch dự phòng
- Ứng cứu sự cố
- Khắc phục thảm họa
- Tính liên tục nghiệp vụ
- Quản lý khủng hoảng
- **Kiểm tra kế hoạch dự phòng**
- Câu hỏi ôn tập

Kiểm tra kế hoạch dự phòng…

- Tất cả các kế hoạch phải được kiểm tra để xác định các lỗ hổng, lỗi và các quy trình không hiệu quả.
- Một số chiến lược kiểm tra có thể được sử dụng để kiểm tra các kế hoạch dự phòng:

1. Kiểm tra tại bàn
2. Duyệt qua có cấu trúc
3. Mô phỏng
4. Kiểm tra toàn bộ gián đoạn.

Kiểm tra kế hoạch dự phòng…

- Tiến hành các buổi hướng dẫn định kỳ (hoặc các buổi nói chuyện) về từng kế hoạch thành phần CP
- Cập nhật các kế hoạch này khi doanh nghiệp và các nguồn thông tin của nó thay đổi
- Quá trình kiểm tra nên đào tạo mọi người để đảm nhận trong trường hợp không có trưởng nhóm hoặc thành viên không thể thiếu của nhóm thực thi.

Kiểm tra kế hoạch dự phòng…

- Cải tiến quy trình liên tục:
  - Mỗi lần tổ chức diễn tập các kế hoạch, tổ chức cần rút kinh nghiệm trong quá trình này, cải tiến các kế hoạch và sau đó diễn tập lại.
  - Mỗi khi một sự cố hoặc thảm họa xảy ra, tổ chức nên xem xét lại những gì đã làm đúng và sai.
  - Các kết quả thực tế cần được phân tích kỹ lưỡng đến mức bất kỳ thay đổi nào đối với kế hoạch có thể dẫn đến kết quả cải thiện sẽ được thực hiện thành một bộ kế hoạch sửa đổi.
  - Thông qua đánh giá và cải tiến liên tục, tổ chức tiếp tục tiến lên và liên tục cải tiến quy trình để có thể cố gắng đạt được kết quả tốt hơn nữa.

XÂY DỰNG KẾ HOẠCH ỨNG CỨU SỰ CỐ KHẨN CẤP

- Kế hoạch ứng cứu sự cố khẩn cấp
- Ứng cứu sự cố
- Khắc phục thảm họa
- Tính liên tục nghiệp vụ
- Quản lý khủng hoảng
- Kiểm tra kế hoạch dự phòng
- **Câu hỏi ôn tập**

Câu hỏi cuối chương…

- Câu 1. Trình bày các thành phần chính của kế hoạch dự phòng.
- Câu 2. Liệt kê quy trình CP gồm bảy bước do NIST đề xuất.
- Câu 3. Liệt kê và mô tả các đội thực hiện lập kế hoạch và thực hiện các kế hoạch và quy trình CP. Vai trò chính của mỗi loại là gì?
- Câu 4. Liệt kê và mô tả các tiêu chí được sử dụng để xác định xem một sự cố thực sự có đang xảy ra hay không.

Câu hỏi cuối chương…

- Câu 5. Liệt kê và mô tả các bộ thủ tục được sử dụng để phát hiện, ngăn chặn và giải quyết một sự cố.
- Câu 6. Liệt kê và mô tả một số chiến lược ngăn chặn được đưa ra trong văn bản điện tử. Họ tập trung vào những nhiệm vụ nào?
- Câu 7. Kế hoạch phục hồi sau thảm họa là gì, tại sao nó lại quan trọng đối với tổ chức?
- Câu 8. Kế hoạch liên tục trong kinh doanh là gì, tại sao nó lại quan trọng?
- Câu 9. Phân tích tác động kinh doanh là gì và được sử dụng để làm gì?
- Câu 10. Tại sao kế hoạch liên tục phải được thử nghiệm và diễn tập?

Câu hỏi cuối chương…

- Câu 11. Những loại tổ chức nào có thể sử dụng một CP thống nhất? Những loại tổ chức nào có thể sử dụng các thành phần lập CP khác nhau làm các kế hoạch riêng biệt? Tại sao?
- Câu 12. Những chiến lược nào có thể được sử dụng để kiểm tra các CP?
- Câu 13. Liệt kê và mô tả hai lựa chọn thay thế chuyên biệt không thường được sử dụng như một chiến lược BC.

Câu hỏi cuối chương…

- Bài 1: Truy cập http://csrc.nist.gov. Trong "Publications", hãy chọn Special Publications, sau đó tìm "SP 800-34, Contingency Planning Guide for Information Technology Systems, June 2002“. Tải xuống và xem lại tài liệu này. Tóm tắt những điểm chính.
- Bài 2: Sử dụng công cụ tìm kiếm trên Web, hãy truy cập một trong những trang web phục hồi sau thảm họa/tính liên tục của doanh nghiệp, như www.disasterrecoveryworld.com, www.drj.com, www.drie.org, www.drii.org hoặc csrc.nist .gov. Tìm kiếm các cụm từ *hot site, warm site* và *cold site*. Các mô tả được cung cấp có khớp với những mô tả của chương này không? Tại sao hoặc tại sao không?

Câu hỏi cuối chương

- Bài 3: Sử dụng định dạng được cung cấp trong văn bản, thiết kế một kế hoạch ứng phó sự cố cho máy tính tại nhà của bạn. Bao gồm các hành động cần thực hiện nếu mỗi sự kiện sau đây xảy ra:
  - Cuộc tấn công của vi rút
  - Mất điện
  - Lửa
  - Đường ống nước nổ
  - ISP thất bại

  Những tình huống nào khác mà bạn nghĩ là quan trọng để lập kế hoạch?

HỌC VIỆN KỸ THUẬT MẬT MÃ
AN TOÀN THÔNG TIN

Thank You!