Chương 9:
An toàn vật lý
(Physical security)

Khoa Khoa học và Kỹ thuật Máy tính
Đại học Bách Khoa Tp.HCM

Nội dung

1. Giới thiệu về an toàn vật lý
2. Các mối nguy hiểm vật lý
3. Kiểm soát an toàn vật lý
4. Quản lý con người

Giới thiệu về an toàn vật lý

- An toàn vật lý (Physical Security) là việc bảo vệ phần cứng, hệ thống mạng, chương trình và dữ liệu khỏi các mối nguy hiểm vật lý có thể gây ảnh hưởng đến hoạt động của hệ thống.
  - Ví dụ: hỏa hoạn có thể gây tổn hại đến các máy tính và hệ thống mạng.
- Trung tâm dữ liệu (data center): nơi tập trung lưu trữ và xử lý dữ liệu, và cần được bảo vệ nghiêm ngặt khỏi các mối nguy hiểm.
- Cần xác định tất cả các mối nguy hiểm và lên kế hoạch để quản lý chúng

Nội dung

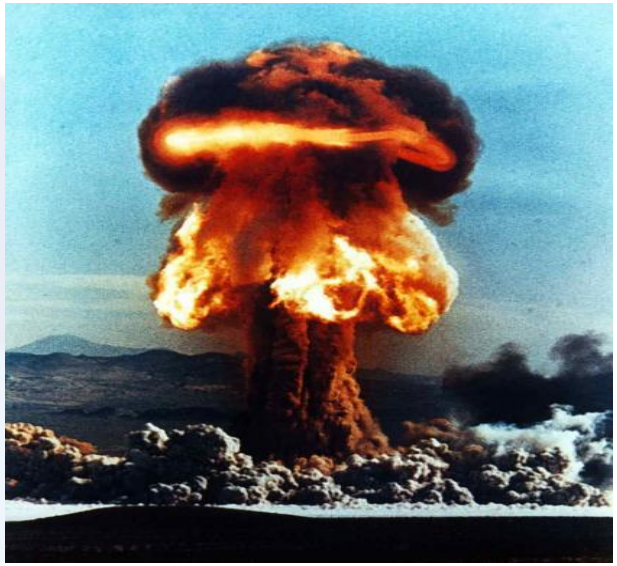
1. Giới thiệu về an toàn vật lý
2. Các mối nguy hiểm vật lý
3. Kiểm soát an toàn vật lý
4. Quản lý con người

Giới thiệu về an toàn vật lý

- Các mối nguy hiểm vật lý gồm:
  - Hỏa hoạn và cháy nổ
  - Nhiệt độ và độ ẩm
  - Thiên tai: ngập lụt, bão, sấm chớp, động đất
  - Sập nhà
  - Hóa chất
  - Mất điện
  - Mất tín hiệu liên lạc
  - Thiết bị hỏng
  - Các phần tử phá hoại: nhân viên bên trong, kẻ trộm

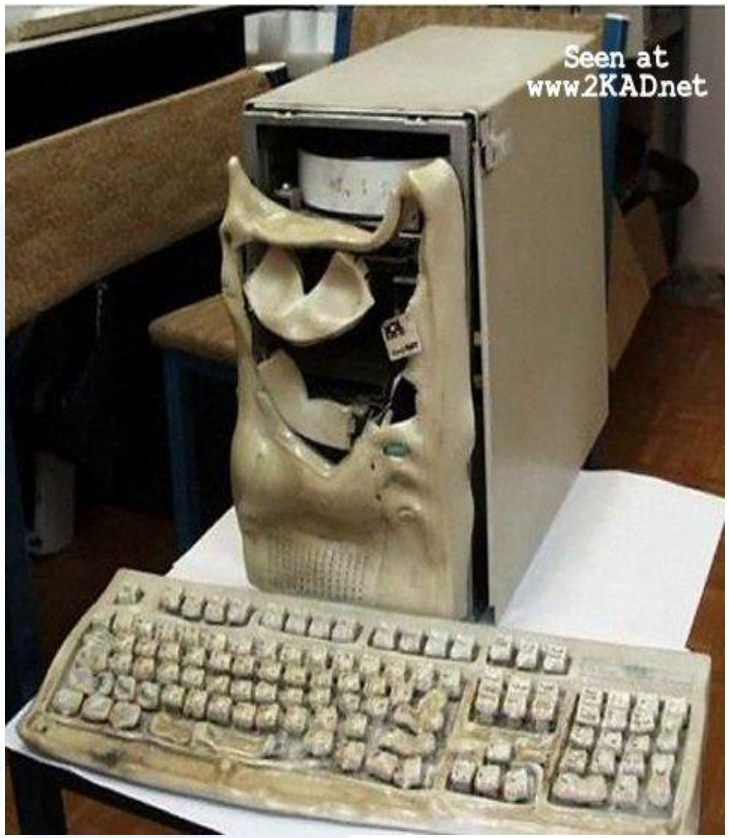
Hỏa hoạn và cháy nổ

- Hỏa hoạn và cháy nổ sẽ gây hư hỏng toàn bộ hệ thống và dữ liệu
- Có hệ thống phát hiện hỏa hoạn.
- Luôn có sẵn thiết bị chữa cháy và phải kiểm tra thiết bị này thường xuyên.
- Cấm hút thuốc trong các khu vực chứa máy móc, thiết bị
- Các vật liệu dễ cháy cần chứa ở phòng riêng



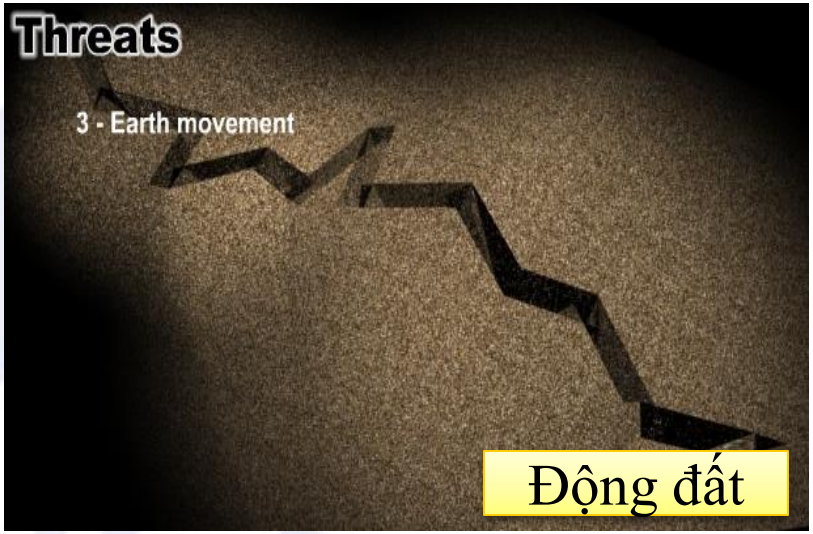
Nhiệt độ và độ ẩm

- Nhiệt độ và độ ẩm không đúng sẽ làm giảm tuổi thọ của thiết bị
- Hệ thống điều hòa được dùng để điều khiển nhiệt độ và độ ẩm.
- Theo ASHRAE (American Society of Heating, Refrigerating and Air Conditioning Engineers) các thiết bị điện tử hoạt động tốt ở nhiệt độ 20–25 °C và độ ẩm 40–60%



Thiên tai


Ngập lụt



Động đất


Sấm chớp


Bão

Sập nhà

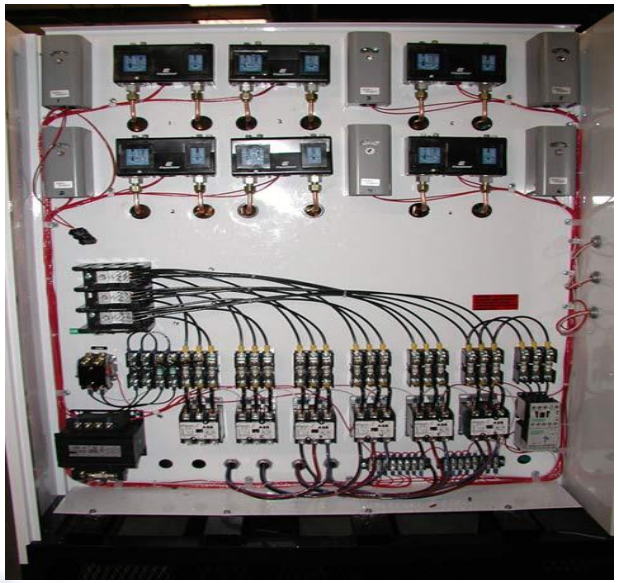
- Máy móc và server chứa dữ liệu quan trọng cần đặt ở những nơi vững chắc

Hóa chất

- Có thể gây biến dạng thiết bị và mất dữ liệu.
- Không đặt gần những hóa chất độc

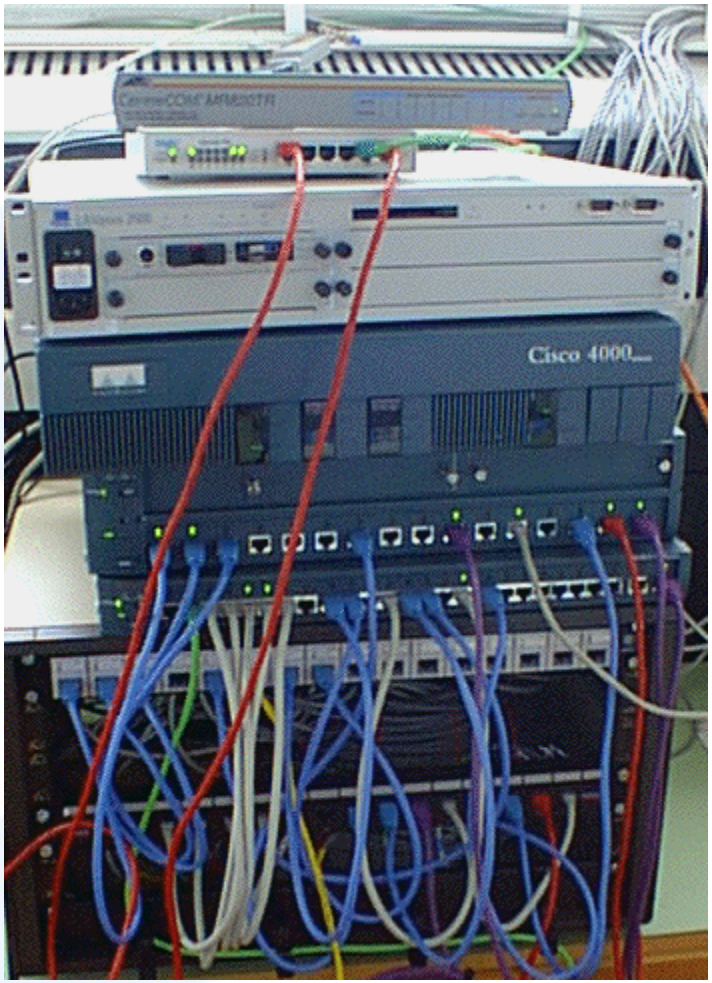
Mất điện

- Đảm bảo nguồn điện 24/24: UPS và máy phát điện.
- Tránh tăng giảm điện áp đột ngột.



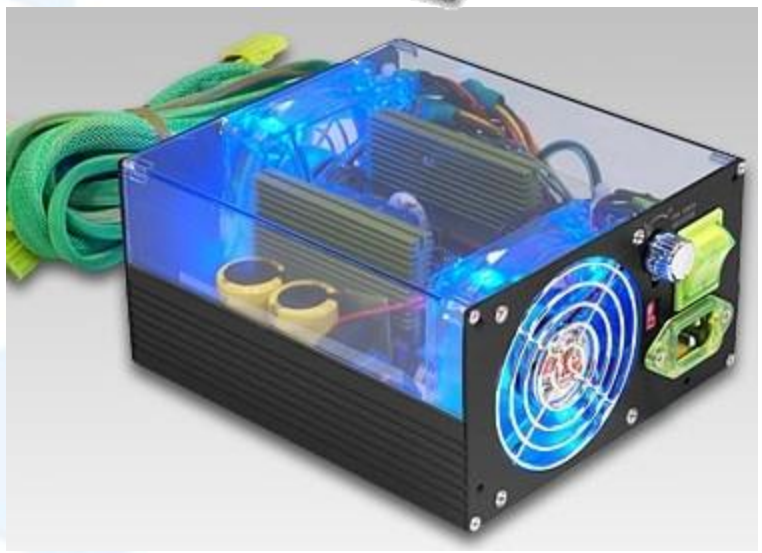
Mất tín hiệu liên lạc

- Mất tín hiệu liên lạc sẽ làm ngưng trệ mọi hoạt động của hệ thống thông tin
- Đảm bảo tín hiệu liên lạc 24/24
- Có hệ thống cáp dự phòng



Thiết bị hỏng

- Sử dụng và bảo trì đúng kỹ thuật
- Thường xuyên back-up dữ liệu



Các phần tử phá hoại

- Kẻ trộm
- Nhân viên phá hoại từ bên trong

Nội dung

1. Giới thiệu về an toàn vật lý
2. Các mối nguy hiểm vật lý
3. Kiểm soát an toàn vật lý
4. Quản lý con người

Kiểm soát an toàn vật lý

- **Quản lý hành chính (Administrative control):** sử dụng các chính sách/luật để định nghĩa cách vận hành hệ thống thông tin đúng, an toàn và bảo mật
- **Quản lý truy cập vật lý (Physical access control)**: sử dụng các công cụ kiểm soát việc ra vào giữa môi trường bên ngoài và hệ thống thông tin như hàng rào, khóa cửa, bảo vệ, …
- **Quản lý kỹ thuật (Technical control)**: sử dụng các phần mềm, phần cứng hỗ trợ bảo vệ an toàn cho các tài sản của công ty/tổ chức

Quản lý hành chính (Administrative control)

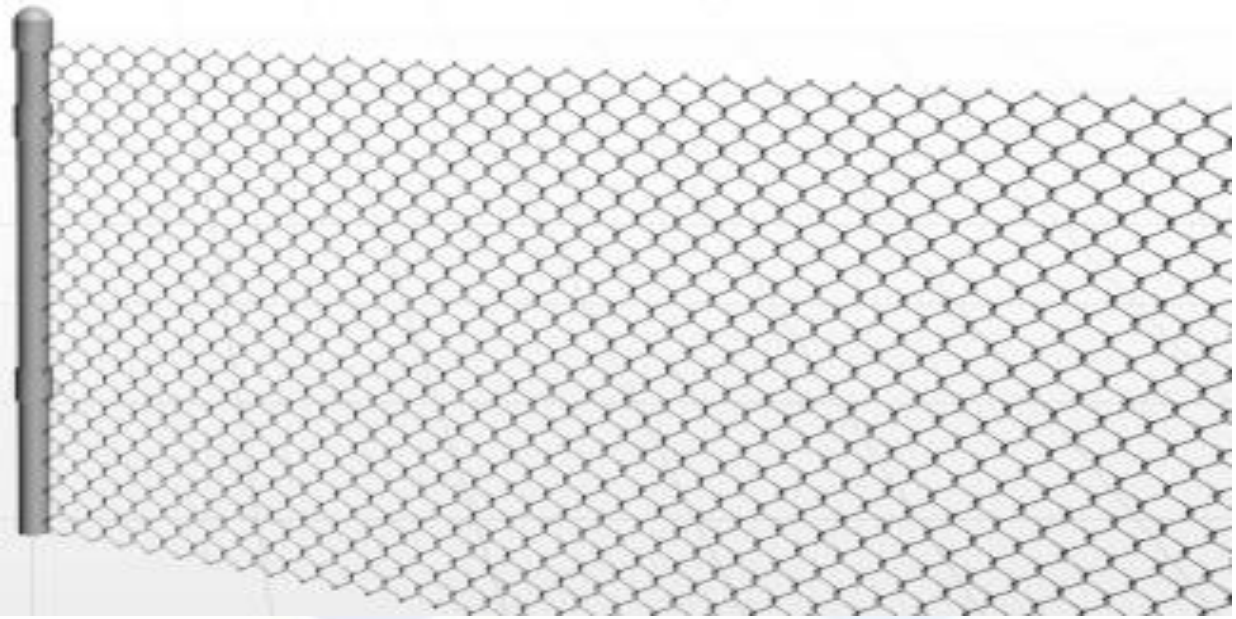
- Lựa chọn vị trí an toàn để xây dựng các trung tâm dữ liệu.
  - Khu vực xung quanh
  - Các yếu tố thiên tai: lũ lụt, động đất, bão,…
- Thiết kế hợp lý và an toàn:
  - Vị trí đặt server CSDL, hệ thống điện, báo cháy
  - Bố trí ánh sáng, cửa ra vào …

Quản lý truy cập vật lý (Physical access control)

- Đảm bảo chỉ có những người có quyền mới được vào các khu vực nhạy cảm như: chỗ server CSDL, hệ thống mạng, điện, …
- Sử dụng các công cụ:
  - Cổng, rào
  - Nhân viên bảo vệ, chó canh
  - Khóa
  - Thiết bị theo dõi, phát hiện các xâm phạm

Cổng, rào

- Hàng rào tạo thành vành đai bảo vệ công ty/tổ chức với môi trường bên ngoài.
- Hàng rào càng cao khả năng chống lại sự xâm phạm càng hiệu quả



Cổng, rào

- Cổng là nơi ra vào công ty/tổ chức do vậy cần kiểm soát kỹ.
- Có thể sử dụng cửa quay (turnstile): một chiều, mỗi lượt ra/vào chỉ có 1 người,

Nhân viên bảo vệ

- Có thể kiểm soát tốt các truy cập vật lý vào hệ thống
- Có thể kết hợp với chó canh.
- Ưu điểm:
  - Linh hoạt khi có thay đổi về môi trường làm việc
  - Có khả năng suy luận và giải quyết vấn đề
- Khuyết điểm:
  - Cần được đào tạo chuyên môn bảo vệ
  - Yếu tố sức khỏe

Khóa

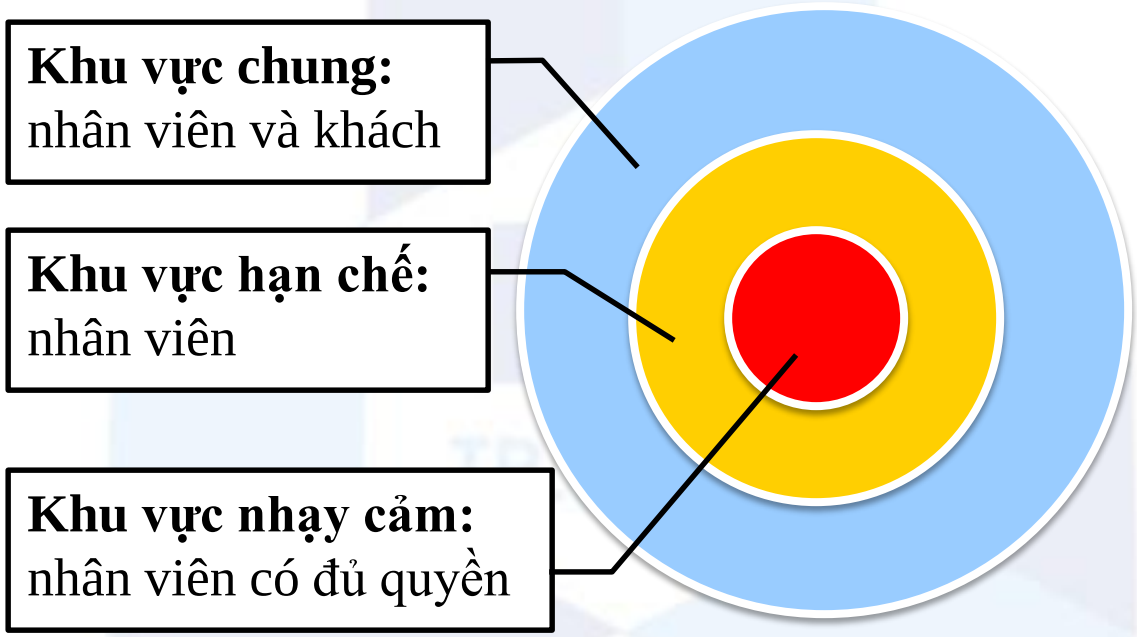
- Khóa và ổ khóa giữ cho cửa, vật chứa được đóng an toàn. Các loại khóa thông minh còn có khả năng định danh và xác thực
- Các loại khóa
  - Khóa thông thường (dùng chìa, mã số)
  - Thẻ thông minh (Smart card)
  - Sinh trắc học

Thiết bị theo dõi, phát hiện xâm nhập

- Hệ thống phát hiện xâm nhập bao gồm các bộ cảm ứng phát hiện chuyển động, thiết bị báo động
  - Khi bộ cảm ứng phát hiện có sự xâm nhập sẽ kích hoạt thiết bị báo động
- Thiết bị theo dõi (như camera) dùng để quan sát hiệu quả các tài sản của công ty/tổ chức:
  - Theo dõi từ xa

Phân vùng

- Phân chia các khu vực trong công ty/tổ chức dựa theo mức độ chứa các thông tin, thiết bị quan trọng.



Phân vùng

Khu vực chung:
nhân viên và khách

Khu vực nhạy cảm:
nhân viên có đủ quyền

Khu vực hạn chế:
nhân viên

Quản lý kỹ thuật (Technical control)

- Thẻ nhân viên
  - Xác thực và định danh
  - Thẻ thông minh: có dải từ tính (magnetic stripe) hoặc con chip lưu thông tin nhân viên. Được dùng trong các thiết bị tự động
  - Thẻ thông thường: lưu thông tin dạng in ấn

Quản lý kỹ thuật

- Phát hiện sự xâm nhập:
  - Kiểm soát truy cập vật lý
  - Hệ thống tự động nhận diện các hoạt động bất thường
- Theo dõi và lưu trữ thông tin truy cập (access log)
  - Theo dõi di chuyển của nhân viên, các thiết bị mà nhân viên đó sử dụng
  - Thẻ thông minh còn có khả năng ghi lại những truy cập của một nhân viên vào một khu vực nhạy cảm

Nội dung

1. Giới thiệu về an toàn vật lý
2. Các mối nguy hiểm vật lý
3. Kiểm soát an toàn vật lý
4. Quản lý con người

Quản lý con người

- Con người là mắc xích yếu nhất trong quá trình bảo mật thông tin.
- Đào tạo tránh rủi ro trong thao tác sai
  - Nhập, sửa, xóa sai dữ liệu
  - Sử dụng các thiết bị không đúng cách: gây sai dữ liệu, hỏng hóc
  - Nhận diện các phần mềm, trang web gây hại
  - Các thao tác cơ bản khi xảy ra lỗi

Quản lý con người

- Trách nhiệm tự quản lý thông tin cá nhân và bảo mật công việc
  - Tự quản máy tính cá nhân, password, thẻ nhân viên, giấy tờ,…
  - Giữ bí mật các công việc nhạy cảm
  - Social engineering
- Tránh kẻ tấn công từ bên trong:
  - Tuyển chọn nhân viên
  - Chính sách đãi ngộ nhân viên
  - Hệ thống theo dõi, chống thoái thác

Nội dung

1. Giới thiệu về an toàn vật lý
2. Các mối nguy hiểm vật lý
3. Kiểm soát an toàn vật lý
4. Quản lý con người


Question ?