TRƯỜNG ĐẠI HỌC NGOẠI THƯƠNG
Hà Nội: Số 91 Chùa Láng, Quận Đống Đa, Hà Nội, Việt Nam - Tel: (84-4) 8344 403 - Fax: (84-4) 8343 605
Cơ sở 2 HCM: Số 15, Đường D5, Phường 25, Quận Bình Thạnh, TP Hồ Chí Minh, Việt Nam
Tel: (84-8) 5127 254 - Fax: (84-8) 5127 255 - Email: cfi@ftu.edu.vn - Website: www.ftu.edu.vn

CHUYÊN ĐỀ:

RỦI RO VÀ PHÒNG TRÁNH RỦI RO TRONG TMĐT

FOREIGN TRADE UNIVERSITY

Hà Nội, 2010

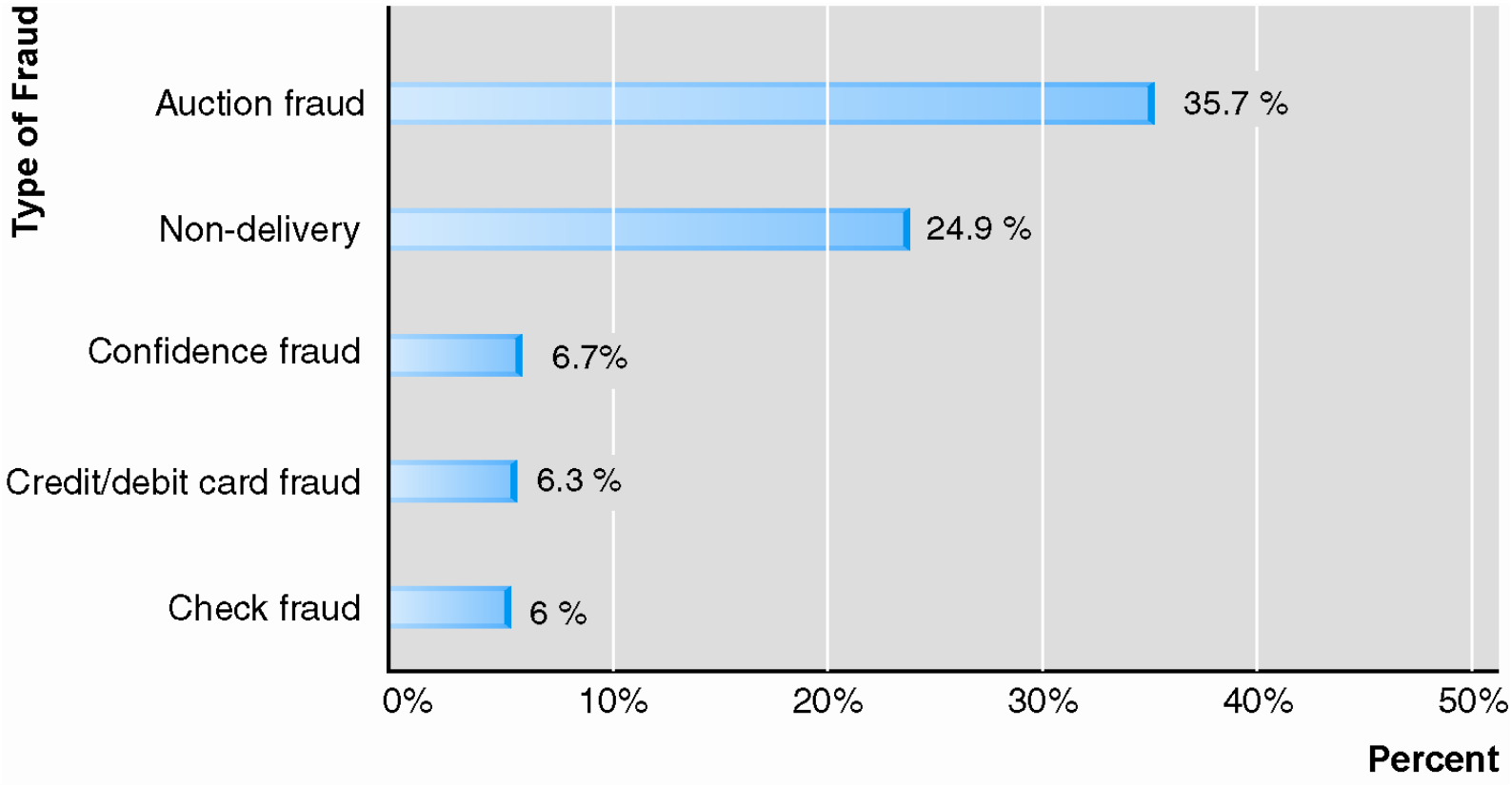
Môi trường an ninh trong TMĐT

- Hiện chưa có con số cụ thể về tội phạm mạng, con số thiệt hại là khá lớn nhưng ổn định, các cá nhân phải đối mặt với nhiều rủi ro gian lận mới có thể liên quan tới tổn thất mà không được bảo hiểm
  - Theo Symantec: lượng tội phạm mạng gia tăng trong năm 2007
  - Theo IC3 (Internet crime complain center): Đã xử lý 200.000 khiếu nại về tội phạm trên Internet
  - Theo điều tra năm 2007 của CSI: có 46% hãng báo cáo dò thấy lỗ hổng an ninh trong năm
  - Thị trường phi pháp chào bán tài khoản ăn cắp đang mở rộng

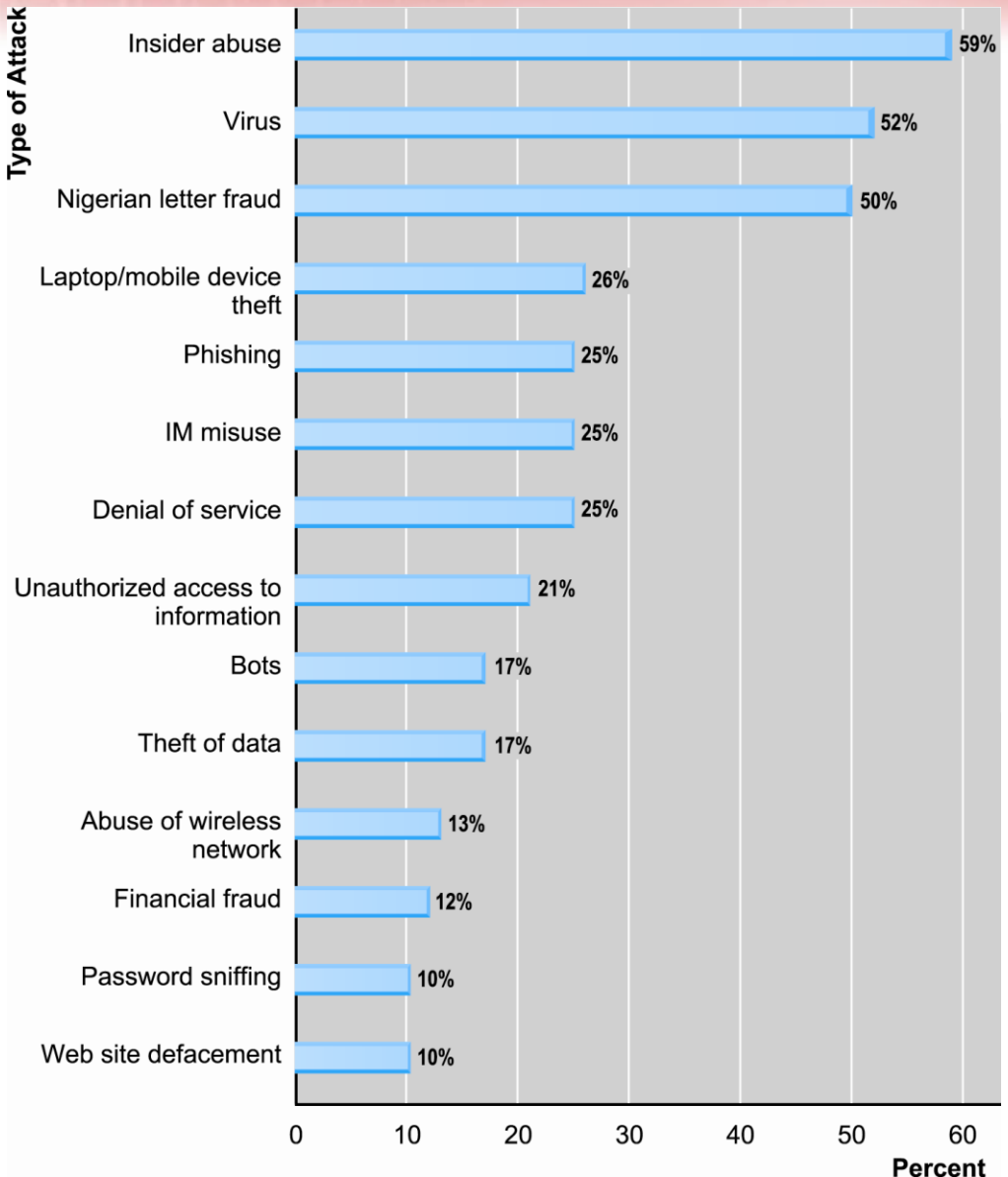
Các rủi ro chính trong TMĐT

- Nhóm rủi ro dữ liệu
- Nhóm rủi ro về công nghệ
- Nhóm rủi ro về thủ tục quy trình giao dịch của tổ chức
- Nhóm rủi ro về luật pháp và các tiêu chuẩn công nghiệp

Các loại tội phạm Internet theo báo cáo của IC3



Các loại hình tấn công hệ thống máy tính



Các loại hình tấn công vào các website TMĐT

- Phát tán virus
- Tin tặc, các chương trình phá hoại
- Phishing – " kẻ giả mạo"
- Kẻ trộm trên mạng (sniffer)
- Tấn công từ chối dịch vụ (DOS - Denial Of Service attack)
- Gửi thư rác với quy mô lớn
- Thu thập thông tin người sử dụng bằng spyware.

Các loại hình tấn công vào các website TMĐT - Phát tán virus

- 3 loại chính:
  - virus ảnh hưởng tới các tệp (file) chương trình (.com, .exe, .bat, .pif, .sys...)
  - virus ảnh hưởng tới hệ thống (đĩa cứng hoặc đĩa khởi động)
  - virus macro
- Virus được đánh giá là mối đe doạ lớn nhất đối với an toàn của các giao dịch thương mại điện tử hiện nay.

Tin tặc (hacker) và các chương trình phá hoại (cybervandalism)

- Tin tặc hay tội phạm máy tính:
  - những người truy cập trái phép vào một website, CSDL hay HTTT.
- Những hành vi của tin tặc:
  - đánh sập website,
  - hủy dữ liệu,
  - xâm nhập hệ thống ngân hàng,
  - đánh cắp các tài khoản ATM,
  - tài khoản Game, tài khoản Mobile

Tin tặc (hacker) và các chương trình phá hoại (cybervandalism)

- Nguy hiểm hơn chúng có thể sử dụng các chương trình phá hoại (cybervandalism) nhằm gây ra các sự cố, làm mất uy tín hoặc phá huỷ website trên phạm vi toàn cầu.

Phishing – " kẻ giả mạo"

- một loại tội phạm công nghệ cao
  - sử dụng email, tin nhắn pop-up hay trang web
  - lừa người dùng cung cấp các thông tin cá nhân như thẻ tín dụng, mật khẩu, số tài khoản ngân hàng.
- Các website thường xuyên bị giả mạo
  - Ebay, MSN, Yahoo, BestBuy, American Online
  - Paypal: http://paypal.com, http://paypal.com@218.36.41.188/fl/login.html

Rủi ro về gian lận thẻ tín dụng

- Trong TMĐT mối đe doạ lớn nhất là bị "mất" (hay bị lộ) các thông tin liên quan đến thẻ tín dụng hoặc các thông tin giao dịch sử dụng thẻ tín dụng trong quá trình thực hiện các giao dịch mua sắm qua mạng và các thiết bị điện tử.

Tấn công từ chối dịch vụ

- tấn công khiến một hệ thống máy tính hoặc một mạng bị quá tải, dẫn tới không thể cung cấp dịch vụ hoặc phải dừng hoạt động.
- Vụ tấn công DOS điển hình vào những website hàng đầu:
  - eBay, Amazon, CNN, E-Trade, Yahoo, Buy.com và ZDNet.

Kẻ trộm trên mạng (sniffer)

- Kẻ trộm trên mạng (sniffer) là một dạng của chương trình theo dõi, nghe trộm, giám sát sự di chuyển của thông tin trên mạng.

Các biện pháp giảm rủi ro trong thương mại điện tử

- Kinh doanh
- Kỹ thuật

Xác định Chủ thể của hợp đồng điện tử

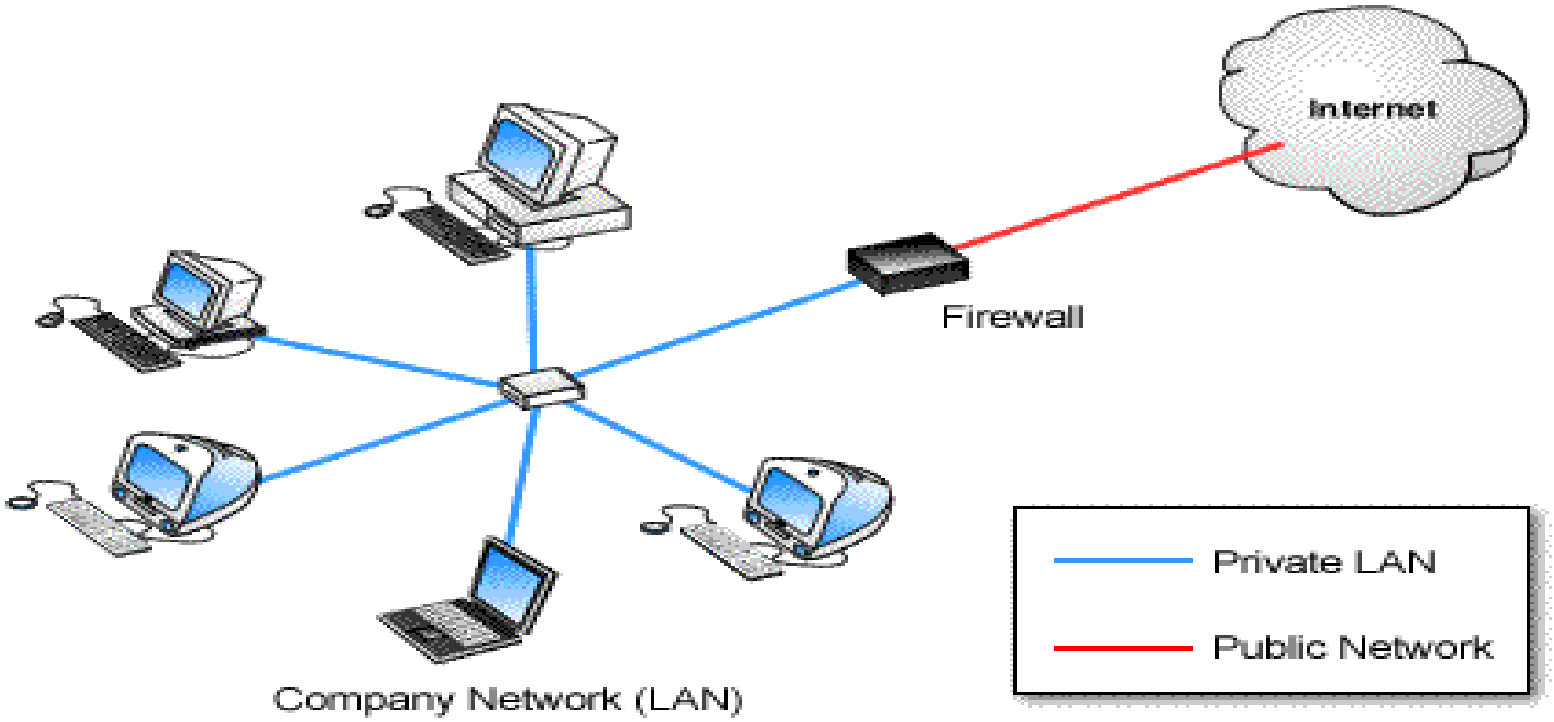
- Trong giao dịch B2C:
  - Uy tín, thương hiệu của chính doanh nghiệp đó
  - Sự xác thực của một cơ quan có uy tín (Bộ thương mại, nhà cung cấp dịch vụ Internet, cơ quan quản lý sàn giao dịch điện tử, Verisign, Trustvn)

Để xác thực khách hàng, doanh nghiệp căn cứ vào:

  - Thông tin thẻ tín dụng
  - Kiểm tra các đơn hàng
  - ID number, địa chỉ, vân tay, giọng nói…
- Trong giao dịch B2B: Các doanh nghiệp xác thực lẫn nhau thông qua:
  - Cơ quan chứng thực khi sử dụng chữ ký sô
  - Thông qua một cơ quan quản lý, tổ chức có uy tín

Một số biện pháp bảo mật trong TMĐT

- Tường lửa: Windows XP Personal firewall, Microsoft ISA server (đa chức năng), Checkpoint



Một số biện pháp bảo mật trong TMĐT

- Tường lửa
- Mạng riêng ảo (VPN)
- Phòng chống virus
- Sử dụng các giải pháp mã hóa
  - Chữ ký số
  - Phong bì số
  - Chứng thư số

Case study

- Vụ tấn công vào Chodientu.com
- Rủi ro trong thương mại điện tử của iPremier

Xin cảm ơn!