SUCCEED TOGETHER

INTERNATIONAL DATA GROUP

SECURITY WORLD 2010
CSO Workshop
23 March 2010 - Hilton Hanoi Opera

Một số kinh nghiệm trong việc xây dựng & thực thi Chính sách bảo mật (CSBM) tại Việt nam

Người trình bày: Ngô Văn Dũng
Giám đốc bộ phận an ninh mạng
Công ty CP Hệ thống thông tin FPT (FPT-IS)

Kinh nghiệm xây dựng CSBM

1. Hiểm họa về mất an toàn thông tin (ATTT) & phương hướng khắc phục
2. Các kinh nghiệm trong việc xây dựng chính sách bảo mật thông tin

Sự phát triển của các hiểm họa mất ATTT

1985-1994 date	1995-1999	2000-2006	2007- Till
• PC Viruses • Floppy disk based	• Internet Viruses, `Worms • E-mail, network `based, Faster `propagation	• Broadband access •Worms, Bots, `Phishing, Spyware • E-mail, network, `Website `transmitted	• Social networking, P2P, Application attacks. • Targeted attacks, Cyber-espionage

Motive: Thrill, Personal satisfaction

Motive: Financial gain

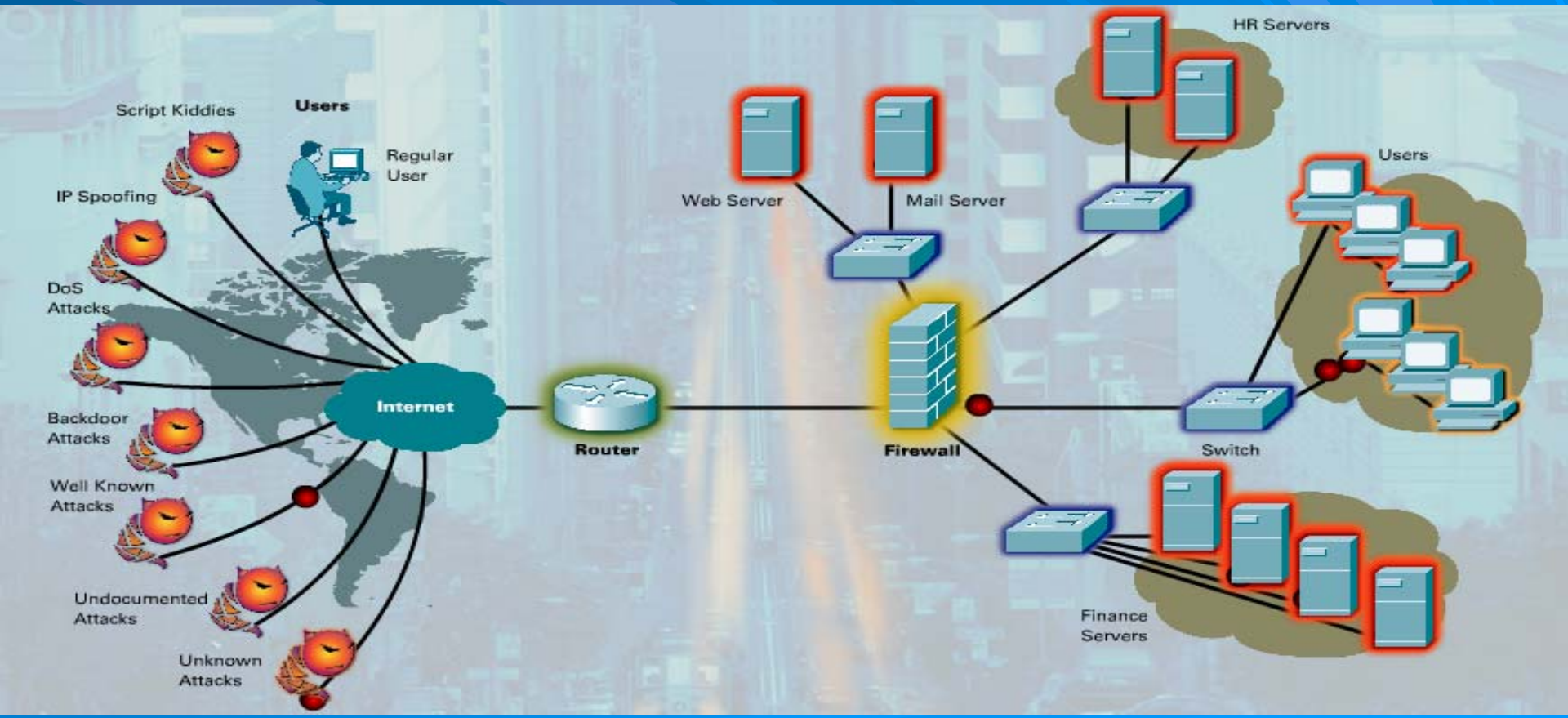
Source: 2008 Frost & Sullivan

Tình hình tội phạm mạng

- Các hoạt động tin tặc liên tục tăng
- Mức độ nguy hiểm ngày một gia tăng, tính tự động ngày càng cao
- Đa dạng về kiểu tấn công
- Xu hướng tấn công vào các tổ chức tài chính, ngân hàng tăng **→Hướng tới lợi nhuận**

Tầm quan trọng của bảo mật thông tin

- Hệ thống thông tin là tài nguyên quan trọng và dễ bị tấn công
- Sự cần thiết phải bảo vệ hệ thống thông tin



Khắc phục các hiểm họa mất ATTT

1. Xây dựng hệ thống an ninh mạng
2. Vận hành & duy trì hệ thống an ninh mạng để đảm bảo ATTT

Xây dựng hệ thống an ninh mạng

Các thành phần cốt yếu của hệ thống an ninh mạng:

- Network Security: Firewall, IPS/IDS
- Endpoint Security: Antivirus, Anti-Spam, NAC
- Xác thực, đảm bảo tính toàn vẹn của dự liệu: OTP, PKI, Mã hóa dữ liệu

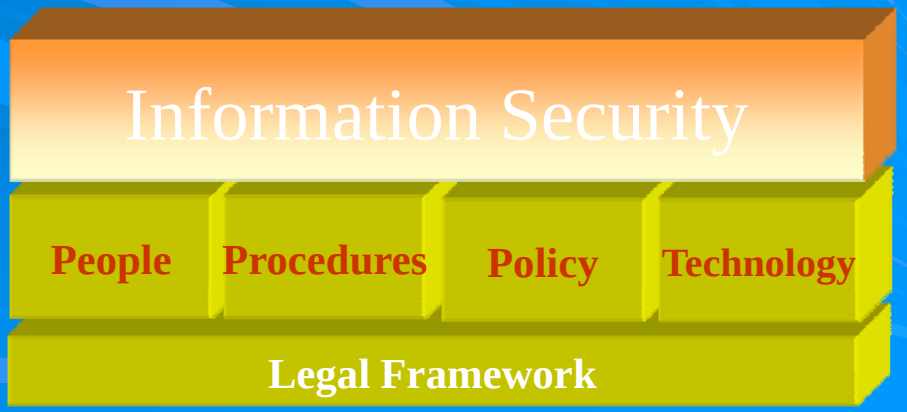
Vận hành & duy trì hệ thống an ninh mạng

- Xây dựng được hệ thống an ninh mạng, chưa có nghĩa là đảm bảo được ATTT trên mạng
- Cần có các biện pháp để vận hành duy trì hệ thống an ninh mạng:
  - Xây dựng nguồn nhân lực để vận hành & duy trì
  - Thường xuyên đánh giá hệ thống an ninh mạng
  - Xây dựng & thực thi CSBM thông tin.

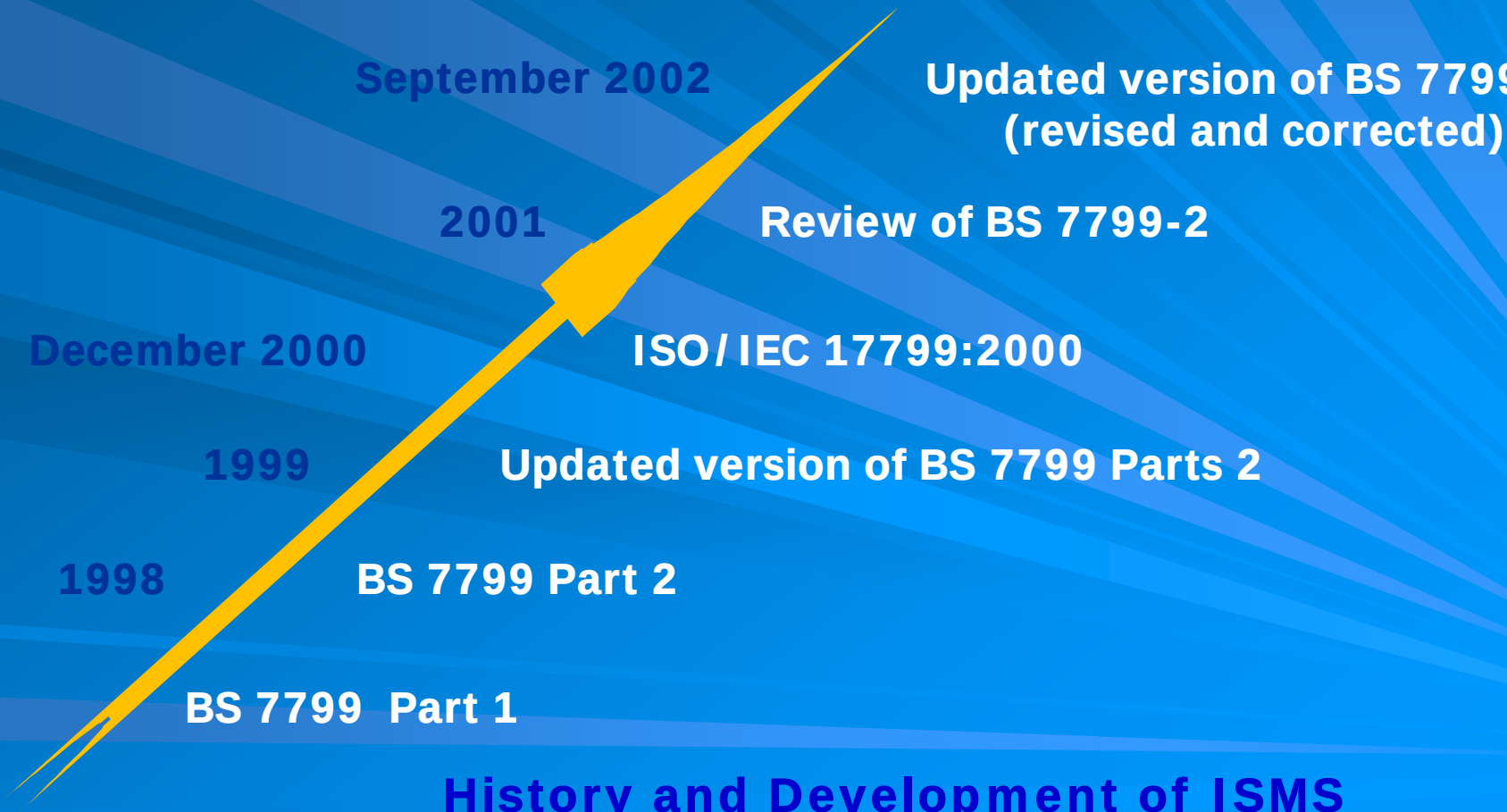
Tổng quan về chính sách bảo mật thông tin

Khái niệm

"Chính sách bảo mật là những tài liệu, đưa ra các mục tiêu an toàn hệ thống cần phải được thực hiện đối với từng vấn đề chính. Nó có vai trò quyết định sử dụng các giải pháp an ninh hệ thống".



Lịch sử phát triển chuẩn ISO 27001



History and Development of ISMS

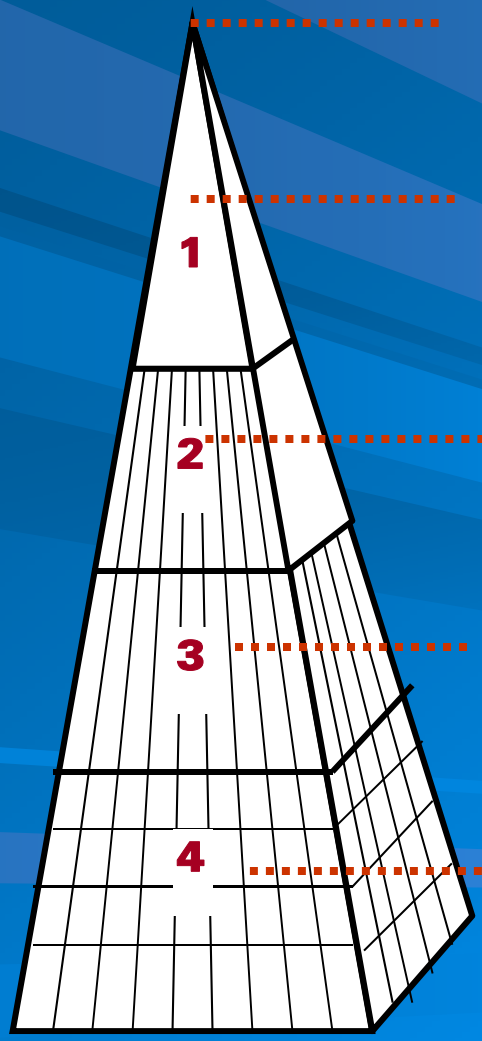
Lịch sử phát triển chuẩn ISO 27001

- 1992: Phòng thương mại và công nghiệp Anh đã cho ra đời "Bộ quy tắc chuẩn cho hoạt động quản lý bảo mật thông tin"
- 1995: Bộ quy tắc trên được chỉnh sửa, bổ sung và tái bản bởi viện chuẩn hóa của Anh với cái tên là BS7799 (part-1)
- 1999: BS7799 được chỉnh sửa, cải tiến lần thứ nhất
- 2000 BS7799 được ISO công nhận và đặt tên là ISO17799
- 2002 BS7799-part 2 ra đời
- 10/2005 BS7799-part 2 được ISO công nhận và đổi thành ISO 27001

Khái niệm về chuẩn ISO 27001

- ISO/IEC 27001 là môt chuẩn quốc tế về quản lý bảo mật thông tin do Tổ Chức Chất Lượng Quốc Tế và Hội Đồng Điện Tử Quốc Tế xuất bản vào tháng 10/2005.
- ISO 27001, với tên đầy đủ là ISO/IEC 27001:2005 đề ra các yêu cầu để thiết lập, triển khai, vận hành, theo dõi, kiểm tra, bảo trì và cải tiến hệ thống quản lý bảo mật thông tin Information Security Management System (ISMS).
- ISO 27001 có thể áp dụng cho tất cả các loại hình tổ chức như các doanh nghiệp, tổ chức tài chính ngân hàng, các cơ quan chính phủ, tổ chức phi lợi nhuận

Tầm quan trọng của chính sách bảo mật



IS Policy, objectives

Security manual

Procedures

Work instructions, checklists, forms, etc.

Records

- Qui định của nhà nước (Chỉ thị 03/2007/CT-BBCVT)
- Chính sách bảo mật đưa ra được cần bảo vệ tài nguyên gì
- Cho phép lãnh đạo quản lý dễ dàng hơn.
- Đưa ra những điểm hạn chế mà cần phải có giải pháp khắc phục
- Đảm bảo công ty sẽ có một chính sách chung.
- Ngăn ngừa vi phạm pháp lý
- Định hướng tăng cường lựa chọn các giải pháp an ninh

Lợi ích khi có CSBM thông tin

- Giảm thiểu được các rủi ro về bảo mật thông tin
- Củng cố năng lực của các tổ chức khi hội nhập quốc tế, nâng cao độ tin cậy & lòng tin của khách hàng và các đối tác
- Doanh nghiệp sẽ tận dụng các cơ hội phát triển và gia tăng quan hệ với khách hàng, đối tác và hình ảnh thương hiệu thông qua việc quảng bá một hệ thống quản lý bảo mật thông tin hoàn chỉnh
- Góp phần củng cố sự tin cậy của khách hàng đối với các dịch vụ, sản phẩm của tổ chức ,doanh nghiệp. Đồng thời giúp tổ chức xây dựng môi trường làm việc ngày càng chuyên nghiệp
- Nâng cao năng lực cạnh tranh của doanh nghiệp, tổ chức tài chính, ngân hàng

Lợi ích khi có CSBM thông tin

- Đạt được chứng chỉ ISO 27001 là một bằng chứng, chứng tỏ rằng HTTT của tổ chức đã và đang được xây dựng, vận hành một cách hiệu quả, giảm thiểu rủi ro và hỗ trợ đắc lực cho doanh nghiệp, tổ chức, giúp cho doanh nghiệp, tổ chức đạt được mục tiêu một cách hiệu quả.

Các bước thực hiện

- Xây dựng ISMS
- Triển khai và vận hành ISMS
- Giám sát, xem xét ISMS
- Nâng cấp ISMS

Một số khó khăn trong quá trình xây dựng CSBM

- Khó khăn xuất phát từ nhận thức chưa đầy đủ về ATTT của các tổ chức đơn vị.
- Khó khăn về vấn đề nguồn lực.
- Chi phí đầu tư
- Khó khăn đảm bảo sự tuân thủ chính sách

ISO 27001 tại Việt Nam

- Trong khi trên thế giới đã có khoảng 25 nghìn đơn vị áp dụng tiêu chuẩn ISO/IEC 27001 về Hệ thống quản lý an toàn thông tin, thì ở Việt Nam đến nay mới chỉ có rất ít doanh nghiệp áp dụng tiêu chuẩn này.
- Công ty CP Hệ thống thông tin FPT (FPT-IS) và FCG Vietnam là 2 công ty Việt Nam đầu tiên đạt chứng nhận ISO/IEC 27001 vào cuối năm 2006 đầu 2007.
- Tương lai của chứng chỉ ISO27001 sẽ thu hút mối quan tâm mạnh mẽ như tiếu chuẩn chất lượng ISO 9000 của những năm 90
- Hiện tai FPT-IS đang tư vấn, phối hợp triển khai xây dựng CSBM thông tin cho nhiều khách hàng, đặc biệt là các khách hàng ngân hàng, TC

Tổng kết

- Các hiểm họa mất an toàn thông tin ngày càng nhiều & nguy hiểm
- Xây dựng hệ thống ATTT là hết sức cấp thiết với các tổ chức doanh nghiệp, để làm được điều này thì việc xây dựng & thực thi CSBM là yếu tố cực kỳ quan trọng

SUCCEED TOGETHER

INTERNATIONAL DATA GROUP

Xin chân thành cảm ơn