TỔNG QUAN AN NINH MẠNG



CÔNG TY CỔ PHẦN CIS | Địa chỉ: Tòa nhà D4/D6, Khu Đô thị mới Cầu Giấy, phường Dịch Vọng, quận Cầu Giấy, Hà Nội. Điện thoại: (+84-4) 3513 3049/50, Fax: (+84-4) 3513 3051

NỘI DUNG

Tình hình an ninh thông tin

Thực trạng

- Nhiều báo điện tử ở VN bị tấn công (3/7 - 6/7)
- Việt Nam đang trở thành điểm tấn công "yêu thích" của các hacker
  - Website bị tấn công:

315

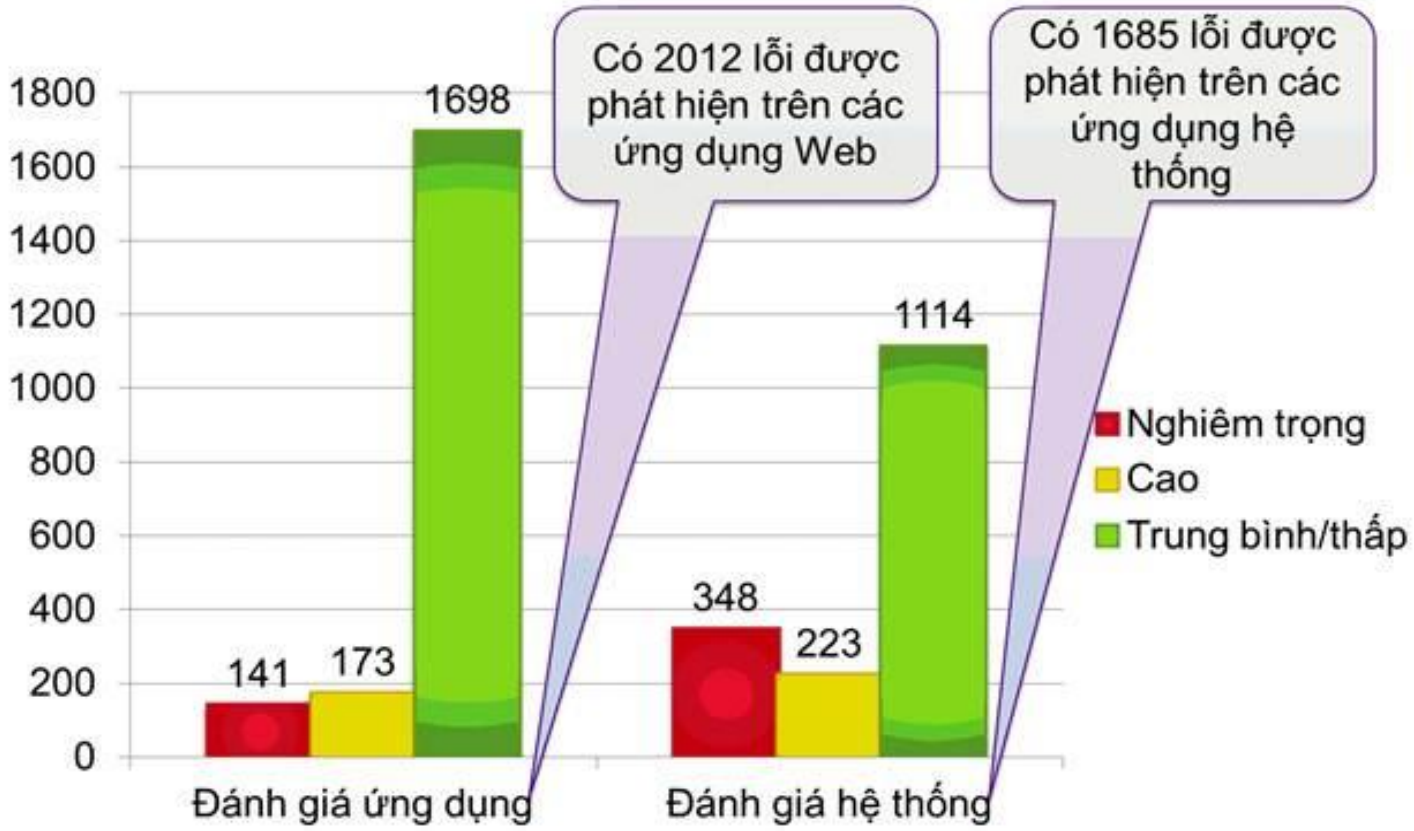
  - Số máy tính bị tấn công: **18/1000** pc
- 2200 website của các cơ quan, doanh nghiệp VN bị tấn công trong năm 2012
  - 100 websites tên miền gov.vn

Số liệu khảo sát, đánh giá

- Việt Nam vẫn tiếp tục có tên trong nhiều danh sách cảnh báo nguy cơ mất an toàn
- Nhiều cơ quan tổ chức phát hiện các kết nối ngầm và các mã độc chuyên dùng để đánh cắp thông tin có chủ đích (APT)
- "Nguy cơ một cuộc chiến tranh mạng đối với Việt nam là có thể xảy ra", Bộ trưởng CA trả lời trước Quốc hội (*Kỳ họp thứ 3, Quốc hội khóa XIII*)

=> Các cuộc tấn công vào mạng thông tin Việt Nam ngày càng mang động cơ chính trị và kinh tế rõ ràng

Khảo sát Website



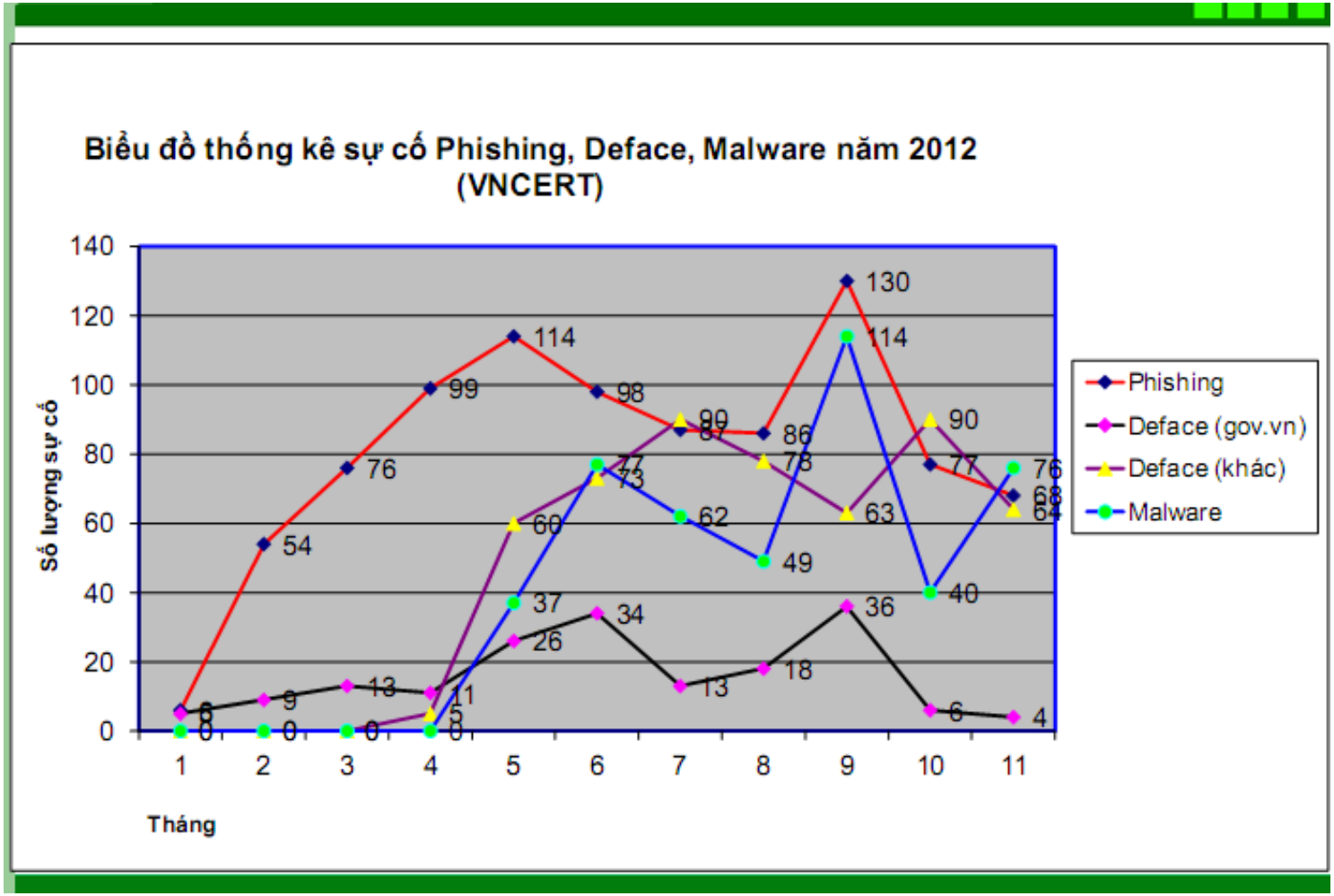
Số liệu thống kê

Phát triển Internet	12/2010 (x triệu)	8/2012 (x triệu)
Số người sử dụng Internet	30.8	31,13
Thuê bao Internet băng rộng	3,64	4,35
Thuê bao điện thoại di động	111,57	135,8
Thuê bao dịch vụ di động 3G	8	16 (5/2012)

Phát triển Chính phủ Điện tử	Bộ, Cơ quan ngang Bộ	Tỉnh, TP trực thuộc TƯ
Có mạng nội bộ và đơn vị chuyên trách CNTT	100%	100%
Có trang, cổng TTĐT	20/22	63/63
Dịch vụ công trực tuyến mức 1-2	3,437	95,002
Dịch vụ công trực tuyến mức 3-4	34	837

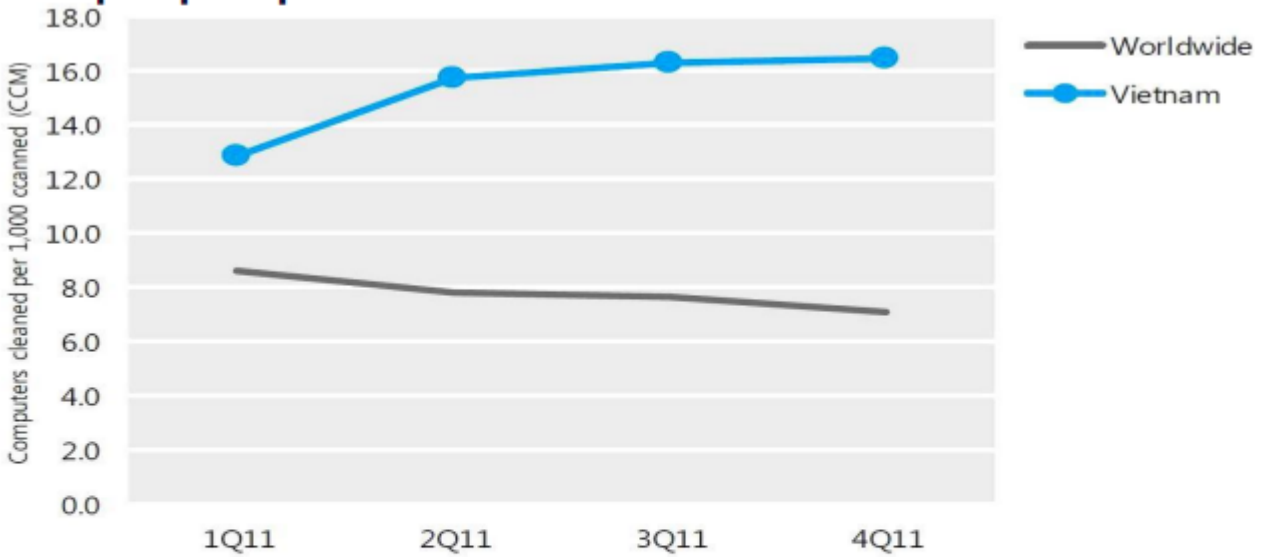
Nguồn: Tổng cục Thống kê

Số liệu thống kê



Số liệu thống kê

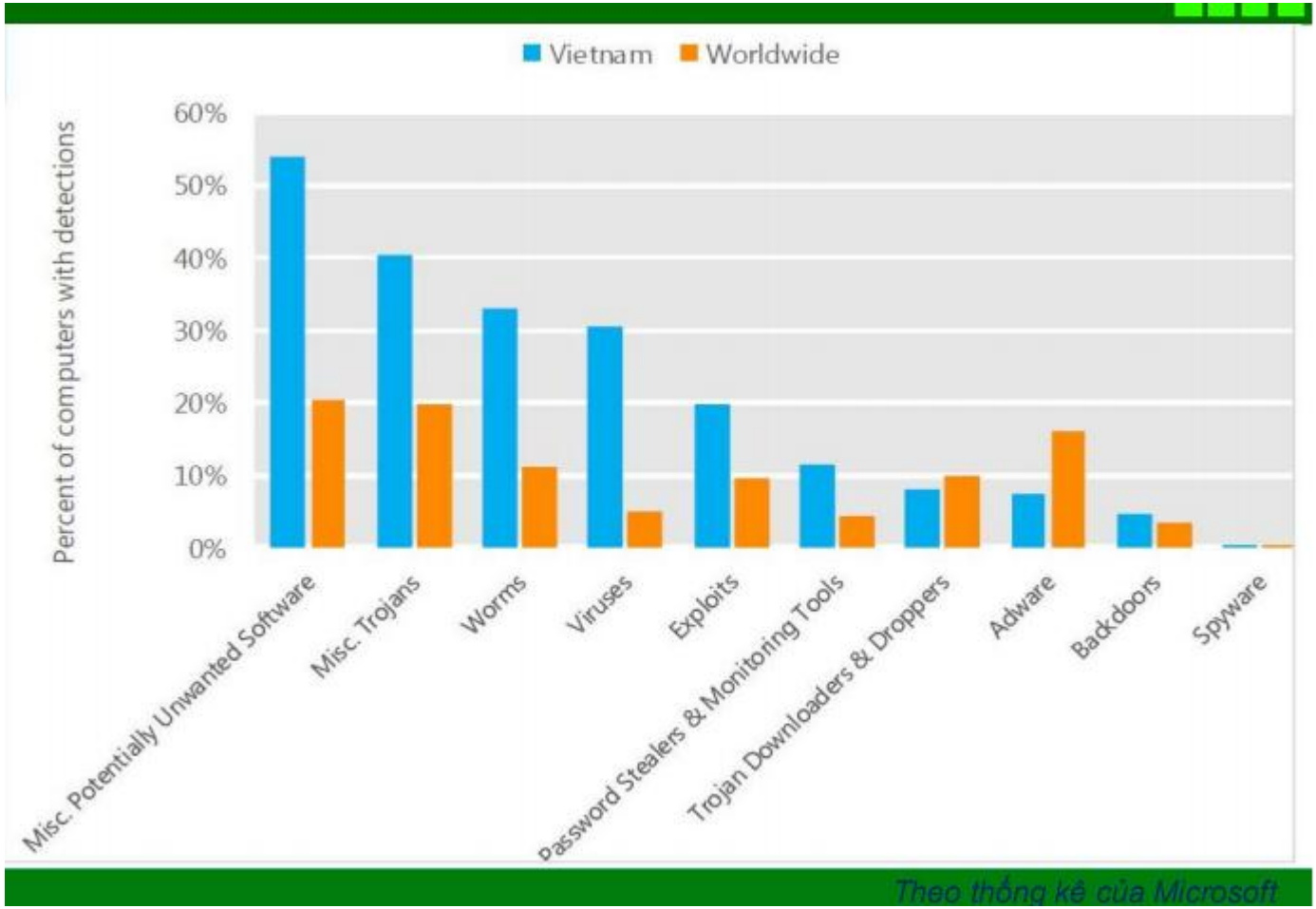
1. Mã độc tại Việt Nam



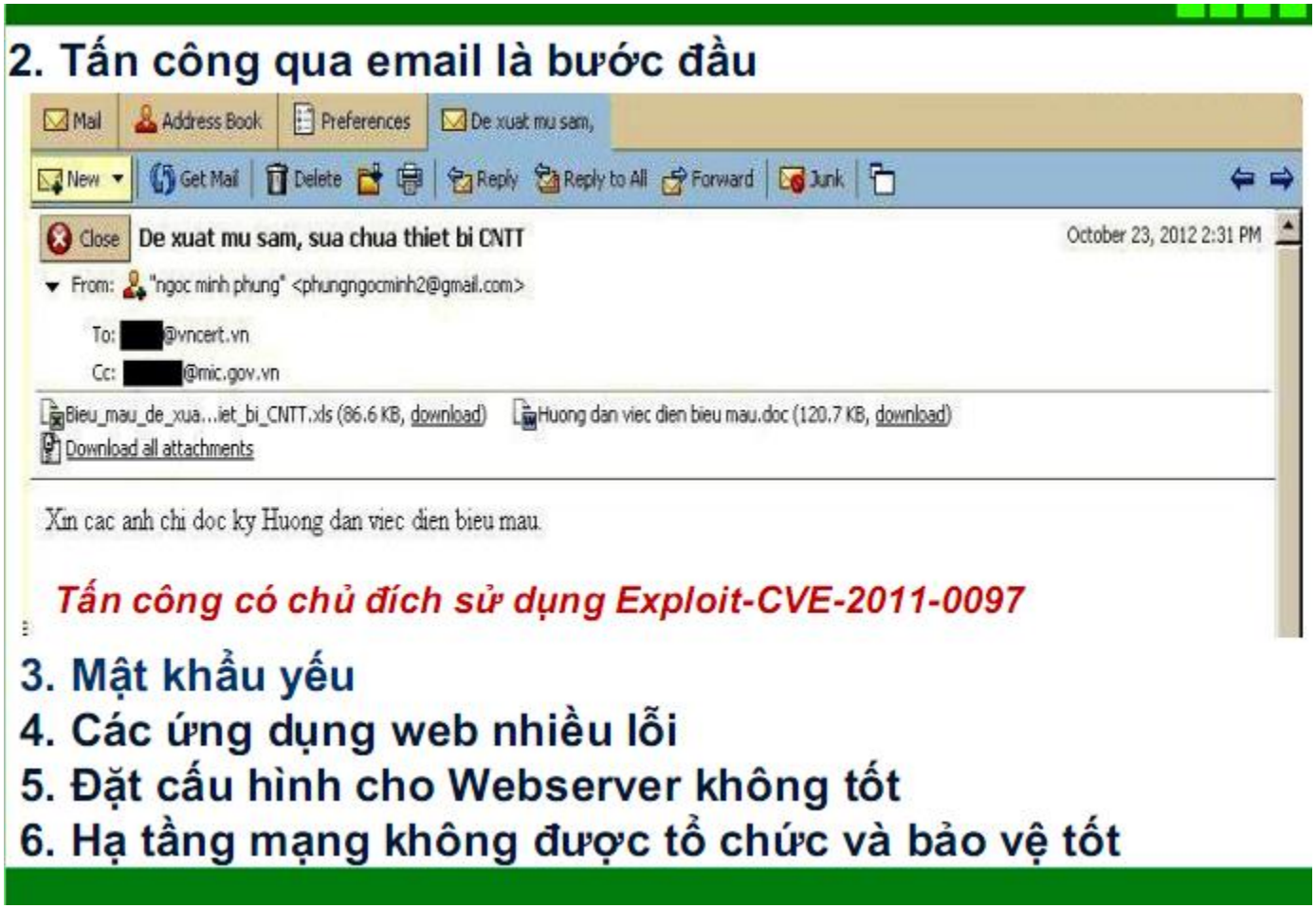
Thống kê Quý 4 năm 2011	Việt Nam	Thế giới
Phát hiện mã độc/1000 lượt kiểm tra	16.5	7.1
Phishing sites / 1000 hosts	0.59	0.02
Malware hosting sites / 1000 hosts	2.83	0.06
Tỷ lệ sites phát tán drive-by downloads	0.061%	3.644%

Theo thống kê của Microsoft

Số liệu thống kê



Số liệu thống kê



Số liệu thống kê

7. Dịch vụ Botnet, spam, mua bán công cụ tấn công

Crimeware tools

Name	Prices (all in US$)	Comments
Phoenix V2.5 (January)	V2.5 mini: $150 V2.5 full: $650	Three new exploits: • JAVA RMI (CVE-2010-0094) • JAVA MIDI (CVE-2010-0842) • JAVA SKYLINE (unknown CVE related to Java OBE)
Bleeding Life V2 reloaded (March)	New buyers: $400 V1 buyers: $250	Includes exploits from 2010: • PDF LIBTIFF: CVE-2010-0188 • JAVA MIDI: CVE-2010-0842 • PDF SWF1: CVE-2010-1297

8. Lấy cắp, mua bán thông tin thẻ ngân hàng, thông tin cá nhân:

a- Tấn công các website bán hàng trực tuyến

b- Sử dụng Keylogger, spyware…

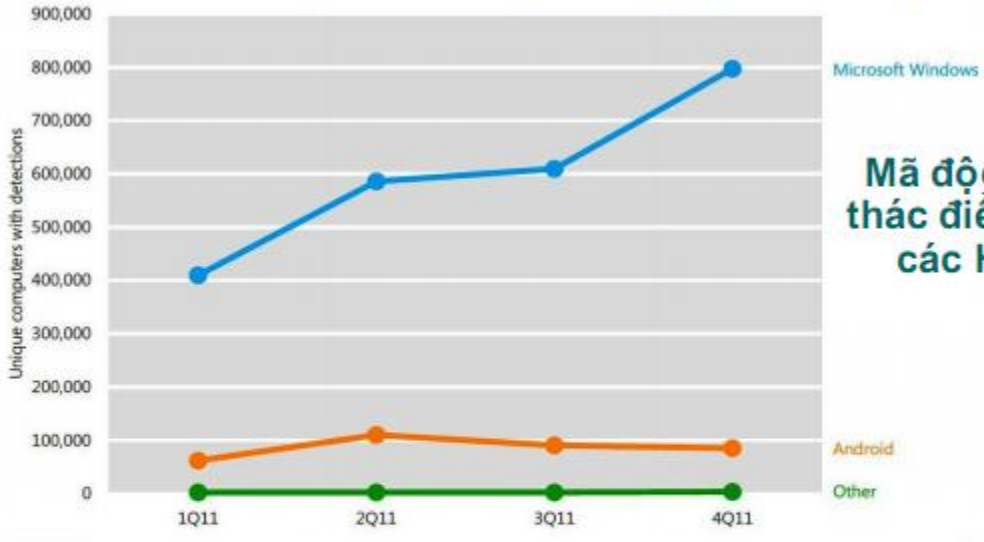
c- Mua bán thông tin thẻ ngân hàng trên mạng (website UG)

d- Phishing

e- Skimming

Số liệu thống kê

9. Mất ATTT đối với thiết bị di động, smart phone



Mã độc khai thác điểm yếu các HĐH

10. Biểu hiện chiến tranh mạng

11. Vấn đề phụ thuộc công nghệ, không kiểm soát được ATTT => Chính sách? Quy trình?

Dự báo

Số lượng các cuộc tấn công sẽ tiếp tục gia tăng, đặc biệt các cuộc tấn công mang màu sắc chính trị (ăn cắp dữ liệu, tình báo, APT...) nhất là khi khả năng "kháng thể" của các website Việt Nam rất yếu.

Nguyên nhân

- Các lỗ hổng bảo mật
- Nhận thức sử dụng, đầu tư cho lĩnh vực an toàn thông tin còn yếu.
- Hệ thống chưa đáp ứng được để có thể phát hiện và ngăn chặn các cuộc tấn công.
- Nhiều website của doanh nghiệp, cơ quan nhà nước còn rất nhiều các lỗ hổng bảo mật.
- Dịch vụ hosting của một số nhà cung cấp chưa thật sự an toàn.

NỘI DUNG

Các nguy cơ an toàn thông tin

Định nghĩa An toàn thông tin

An toàn thông tin nghĩa là gì?

Phải làm gì để đảm bảo an toàn thông tin?

Định nghĩa An toàn thông tin

"Một hệ thống chỉ thật sự an toàn khi tắt điện, rút các phích cắm, bỏ vào két titan khóa lại, rồi chôn trong boongke bê tông, bao phủ bởi khí trơ và được bảo vệ bởi các lính canh có vũ trang và có thù lao hậu hĩnh. Và dù thế, tôi cũng không dám đánh cược cuộc đời mình cho điều đó"

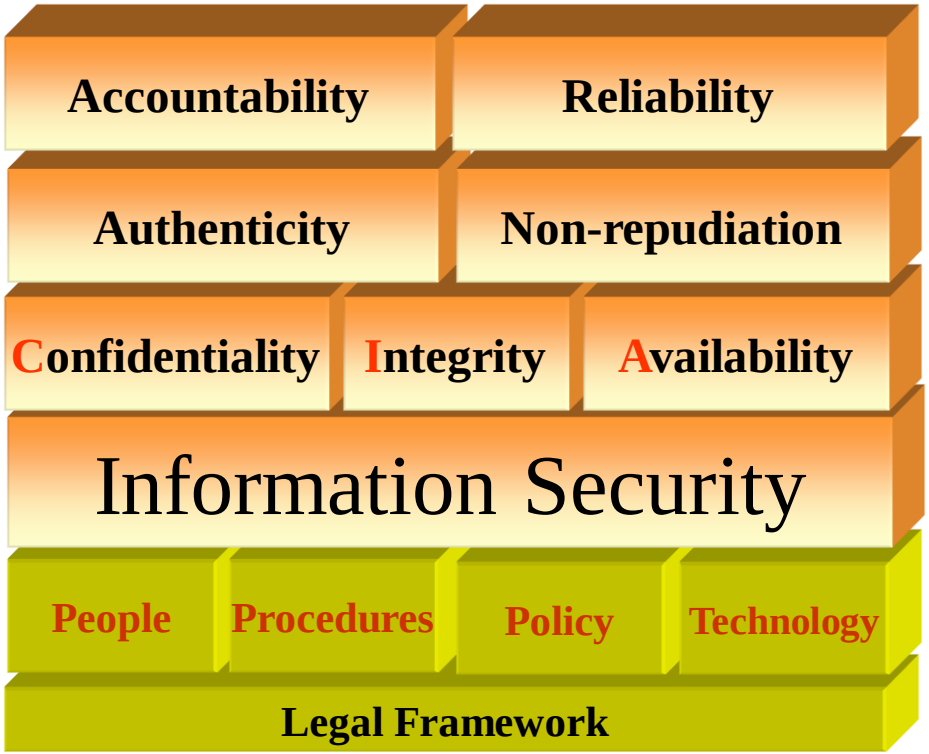
"The only system which is truly secure is one which is switched off and unplugged, locked in a titanium lined safe, buried in a concrete bunker, and is surrounded by nerve gas and very highly paid armed guards. Even then, I wouldn't stake my life on it."

Gene Spafford – Director, Computer Operations, audit, and Security Technology (COAST - Computer Operations, Audit and Security Technology) Purdue University

Định nghĩa An toàn thông tin

An toàn thông tin là các biện pháp nhằm đảm bảo tính bí mật (confidentiality), tính toàn vẹn (integrity) và tính sẵn sàng (availability) của thông tin.

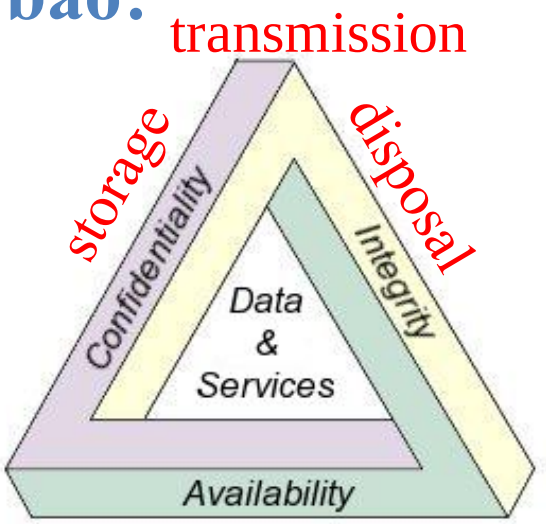
- An toàn an ninh cho hệ thống thông tin không là giải pháp kỹ thuật.
- Cần phải có hành lang pháp lý, quy trình.. để đảm bảo cho an toàn an ninh hệ thống thông tin.



ISO/IEC-27001:2005

Định nghĩa An toàn thông tin

Thông tin trong hệ thống phải đảm bảo:

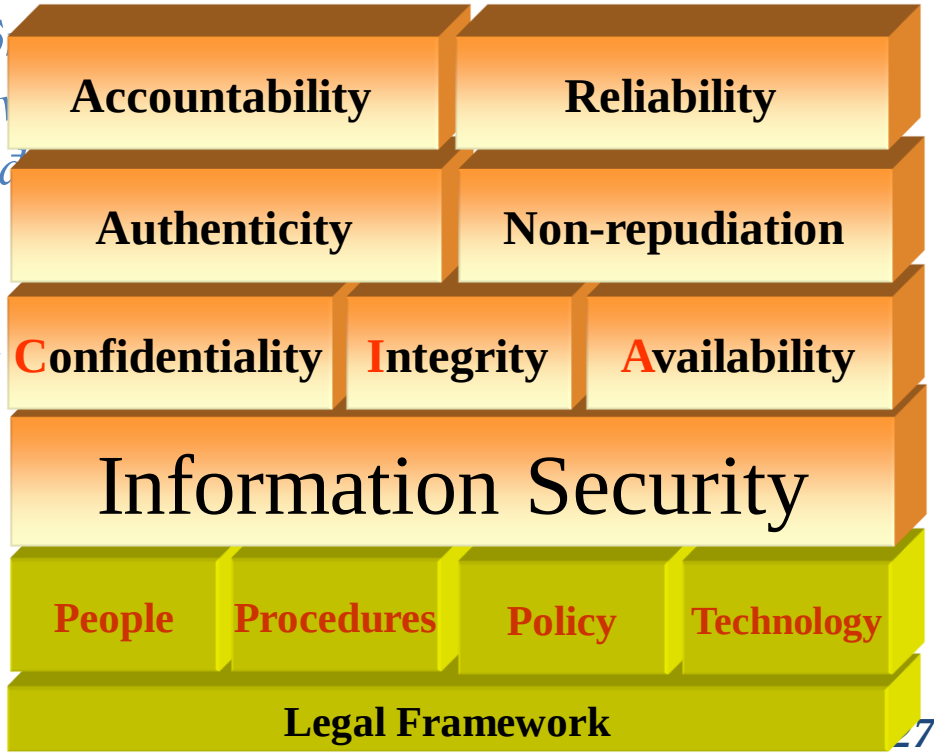


- ***"Tính bí mật":***
  - *Không bị nghe trộm, bị lộ, bị đọc lén trên đường truyền, khi đi qua các hạ tầng truyền thông khác nhau.*
  - *Không bị lộ khi lưu trữ*
- ***"Tính toàn vẹn":***
  - *Thông tin không bị sửa đổi trong khi di chuyển từ nơi phát đến nơi nhận vì bất kỳ lý do gì*
  - *Các lý do khách quan làm thông tin bị sai lệch?*
  - *Các nguyên nhân chủ quan làm thông tin bi sai lệch?*
- ***"Tính sẵn sàng":***
  - *Đảm bảo tính sẵn sàng khi có yêu cầu truy nhập vào bất cứ lúc nào*

Định nghĩa An toàn thông tin

Ngoài ra còn có:

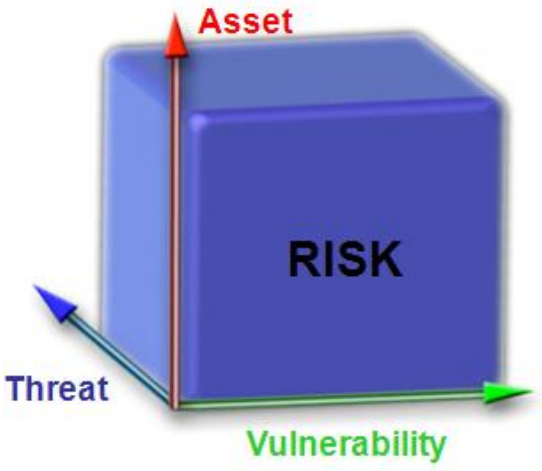
- ***"Chống từ chối":***
  - *Người phát hành thô*
    không thể phủ nhận v
    phát hành hoặc sửa đ
    thông tin
- ***"Tính đáng tin của thông tin"***
- ***"Tính trách nhiệm"***

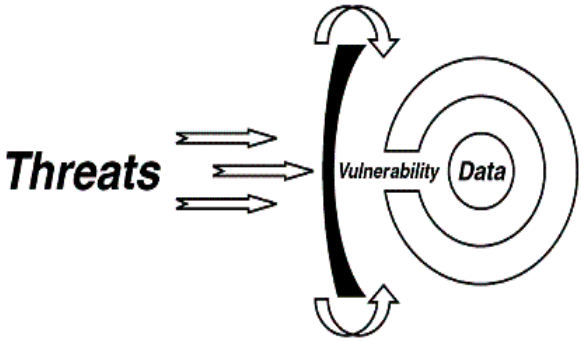


27001:2005

Các nguy cơ, rủi ro

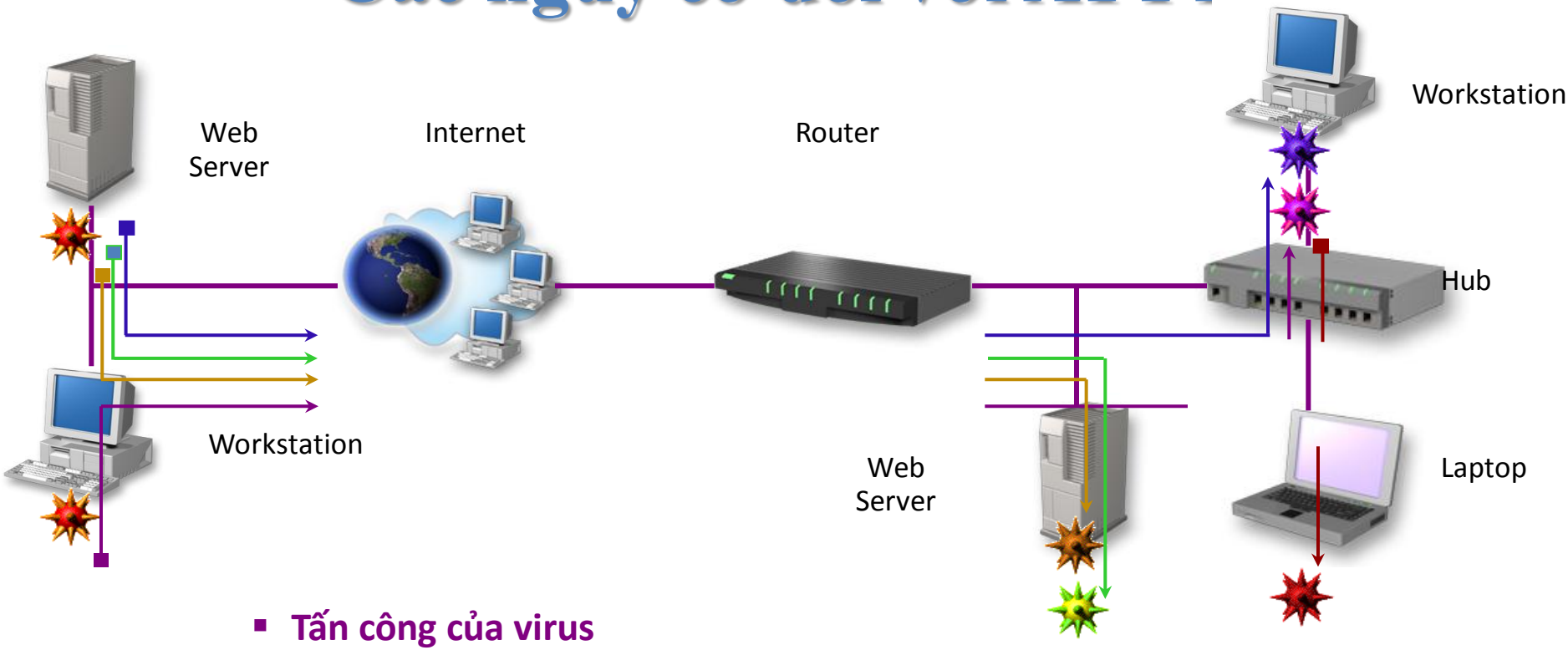
- Risk là gì?
  - Là khả năng một mối đe dọa (Threat) có thể gây hại đến chúng ta.
- Tại sao lại có Risk?
  - Tại vì chúng ta có điểm yếu (Vulnerability) nên Threat mới tạo nên Risk.
- Risk khác Threat và Vulnerability thế nào?
  - Yếu mà ra gió nên bị ốm là Risk (Điểm yếu)
  - Khả năng bị ốm do gió lạnh là Threat (Đe dọa)
  - Yếu nên có khả năng bị ốm là Vulnerability (Lỗ hổng)





RISK= f(Asset,Threat,Vulnerability)

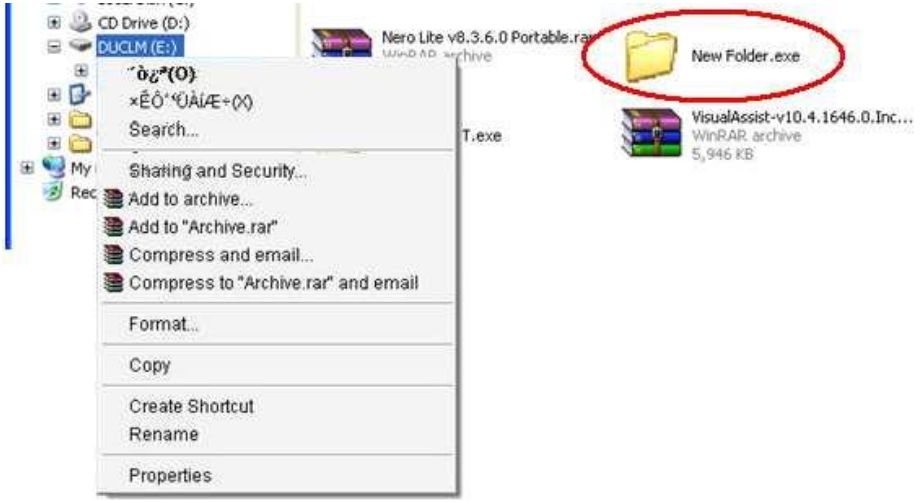
Các nguy cơ đối với ATTT



- Tấn công của virus
- Tấn công của tin tặc (Hacker)
- Tấn công từ chối dịch vụ
- Khai thác các lỗ hổng bảo mật
- Giả mạo, ăn cắp dữ liệu

Virus?

- Khái niệm rộng nhất được đề cập đến là "Malware", được gọi là là "Mã độc hại"
- Mã độc hại được định nghĩa là "một chương trình (program) được chèn một cách bí mật vào hệ thống với mục đích làm tổn hại đến tính bí mật, tính toàn vẹn hoặc tính sẵn sàng của hệ thống"
- Các loại:
  - Worm
  - Trojan Horse
  - Sâu (Worm)
  - Spyware
  - Virus



Phân loại

- Theo NIST mã độc được phân loại như sau:

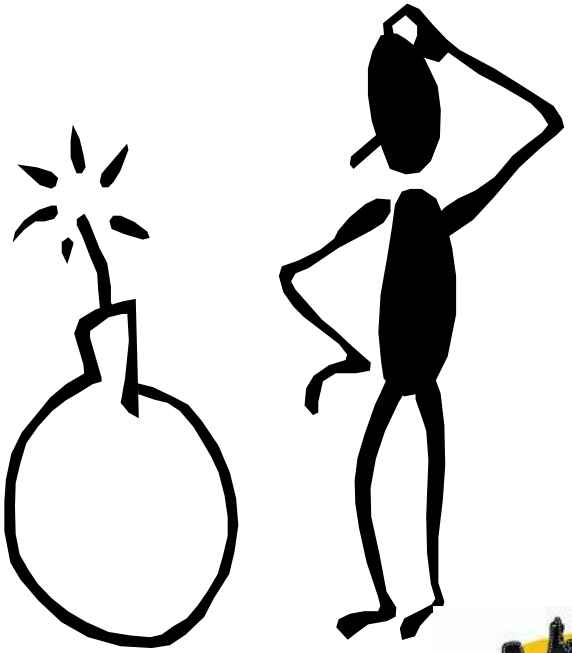
Phân loại			Ví dụ
Mã độc hại (Malware)	**Virus**	Compiled Virus	Michelangelo,Stoned, Jerusalem
		Interpreted Virus	Melisa,
	Worm	Network Service Worm	Sasser
		Mass Mailing Worm	Netsky, Mydoom
	Trojan Horse		
	Maliciuos Mobile Code		Nimda
	Attacker Tool	Backdoor	Trino, Tribe Flood Network
		Keylogger	KeySnatch, Spyster
		Rootkit	LRK5, Knark, Adore, Hack Defender
		Web Browser Plug-in	
		Email Generator	

Các con đường lây lan

- Thiết bị USB, ổ đĩa di động
- Web đen
- Phần mềm crack, keygen
- Email không rõ nguồn gốc
- Các thư mục chia sẻ
- Lỗ hổng phần mềm
- …

Hậu quả

- **Thông tin**
  - Mất tính toàn vẹn
  - Mất tính bí mật
  - Mất tính sẵn sàng
- **Thực tế**
  - Tốn kém chi phí
  - Tốn kém thời gian
  - Ảnh hưởng đến tài nguyên hệ thống
  - Ảnh hưởng danh dự, uy tín của tổ chức
  - Mất cơ hội kinh doanh



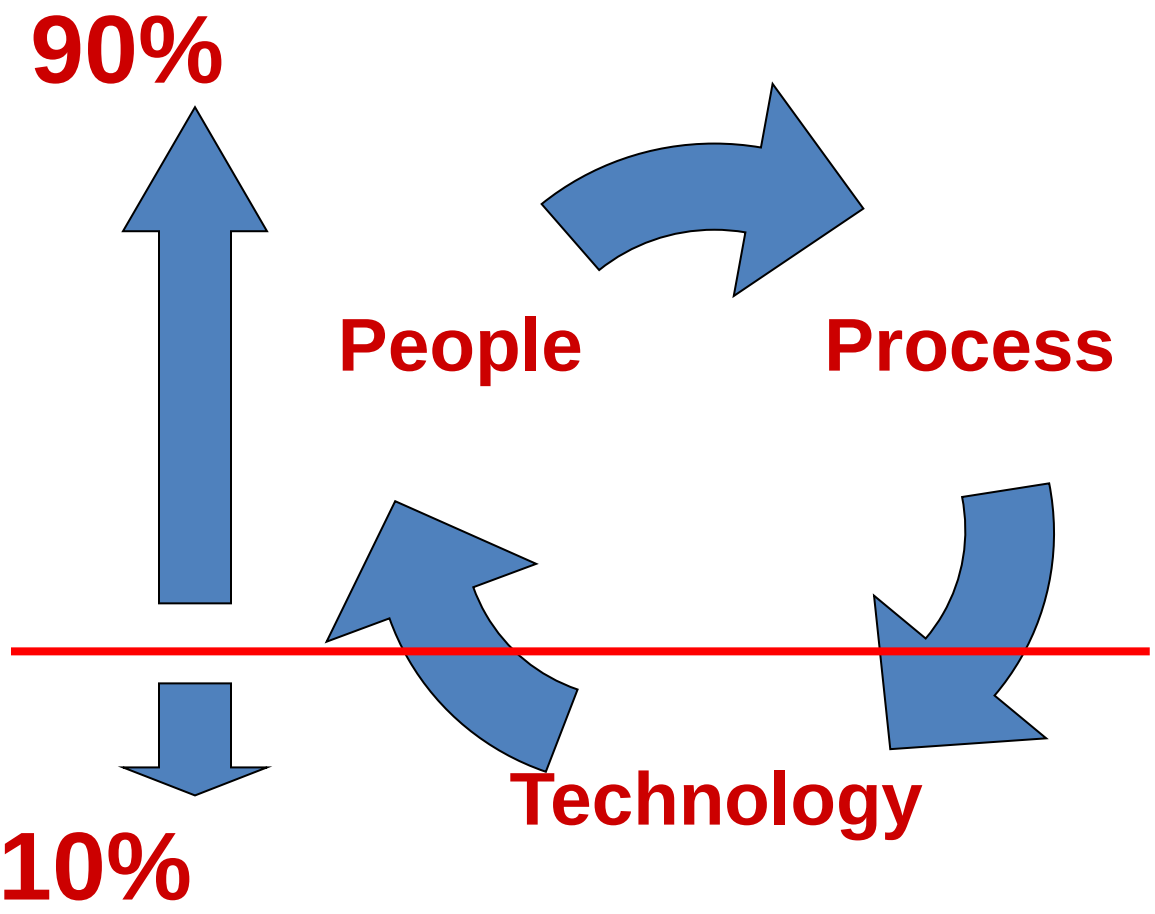
NỘI DUNG

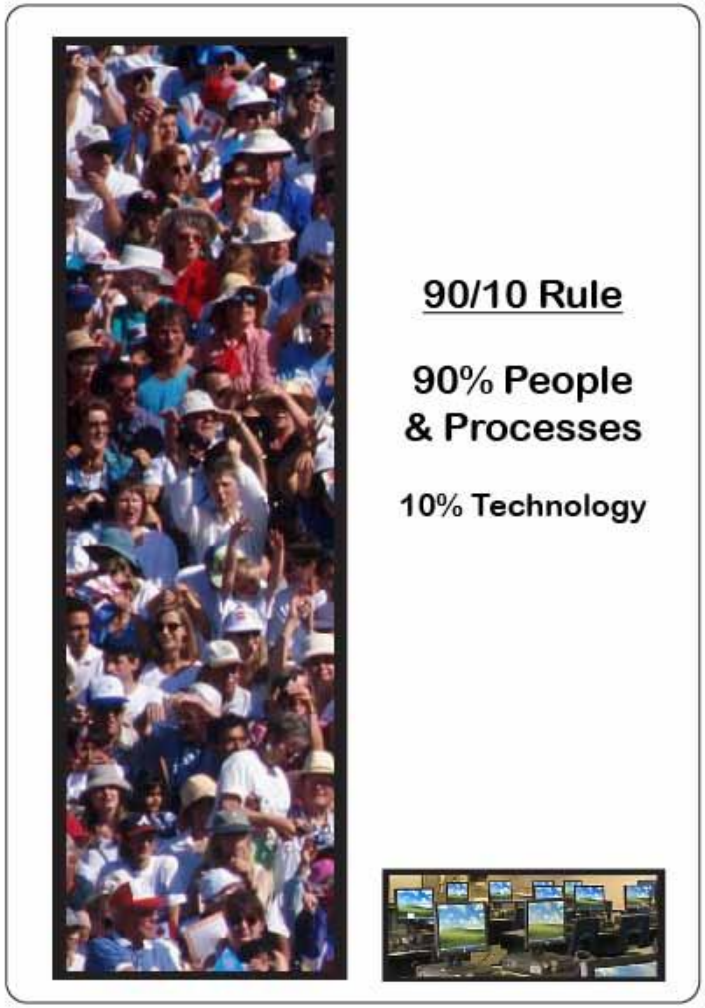
Giải pháp

GIẢI PHÁP

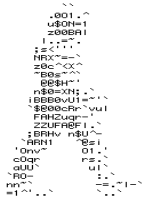
- Cần có sự chuẩn bị nghiêm túc về nhân lực, công nghệ, triển khai đào tạo nâng cao ý thức về an toàn thông tin.
- Nhận thức rõ tầm quan trọng của an toàn thông tin và có kế hoạch tổng thể về an toàn thông tin.
- Cần thường xuyên cập nhật, nâng cấp hệ thống nhằm ứng phó kịp thời với sự thay đổi và tiến bộ công nghệ.

Nhận thức về ATTT?





Nhận thức về ATTT?



Sự nhận thức là sự hiểu biết, kỹ năng và ý thức cá nhân về các quy trình, thiết bị bảo mật thông tin.

Ý thức bảo mật ở đây có thể hiểu rằng một số người cố tình hay vô tình ăn cắp, làm hư hỏng hay lạm dụng quyền hạn của mình làm ảnh hưởng đến hệ thống dữ liệu được lưu trữ trong tổ chức, doanh nghiệp..

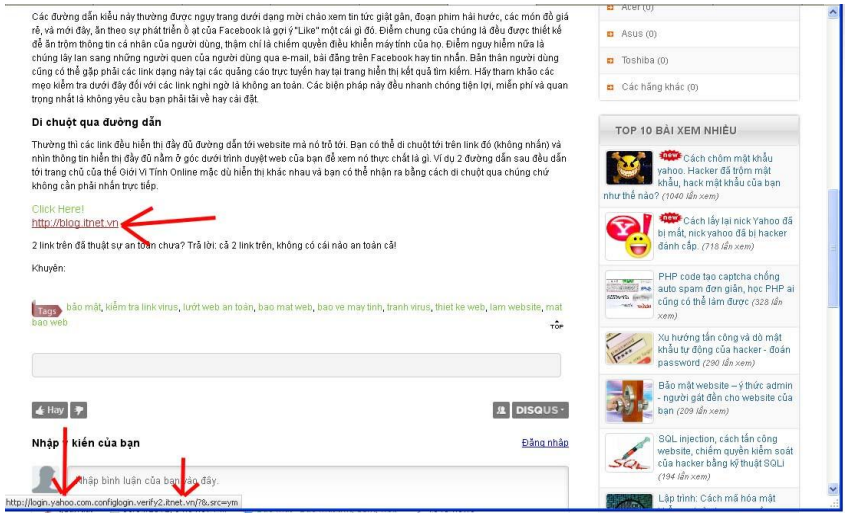
Hung hung: Hi khoe khong?
Hung hung: dao nay` the' nao`?
sonvn: Ừ, vẫn bình thường
sonvn: mấy hôm trước vừa về quê ra
Hung hung: Gai xinh ne , gai xinh ne : http://xrobots.net/Gift/?file=Gaixinh.jpg
Hung hung: ve` duoc may` hom?

Các biện pháp đảm bảo an toàn

- Nhận thức đúng mức về an ninh thông tin
- Thường xuyên cập nhật bản vá các lỗ hổng phần mềm (trình duyệt, email cá nhân…).
- Tạo mật khẩu an toàn
- Mã hóa thông tin quan trọng khi gửi đi
- Kiểm tra kỹ thiết bị di động (USB, CD..)

Các biện pháp đảm bảo an toàn

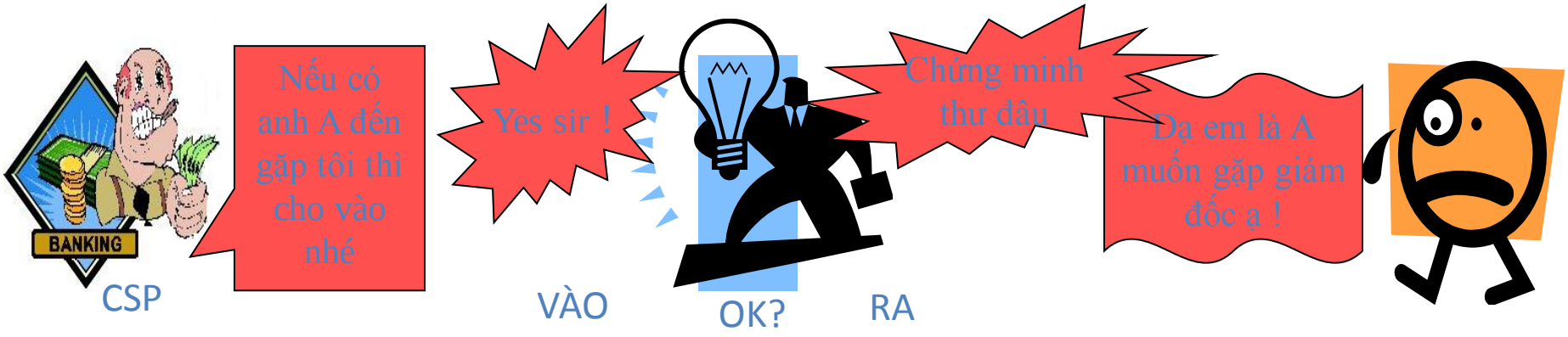
- Click nhưng cần suy nghĩ



- Sử dụng email an toàn
- An toàn với mạng Wifi
- Sử dụng giao thức HTTPS
- Cập nhật bổ sung kiến thức về ATTT

Xác thực

- Authentication



- E- Authentication

User gõ ID, PassWord để truy cập mail

Server xác thực ID, PassWord
để quyết định có cho phép truy cập hay không ?!

Các nhân tố xác thực

- Tính đảm bảo của phương pháp xác thực dựa trên 3 yếu tố cơ bản:
  - Something a person knows (số PIN, mật khẩu)
  - Something a person has (SmartCard, Token…)
  - Something a person is (Những đặc tính sinh trắc học: Vân tay, mống mắt…)

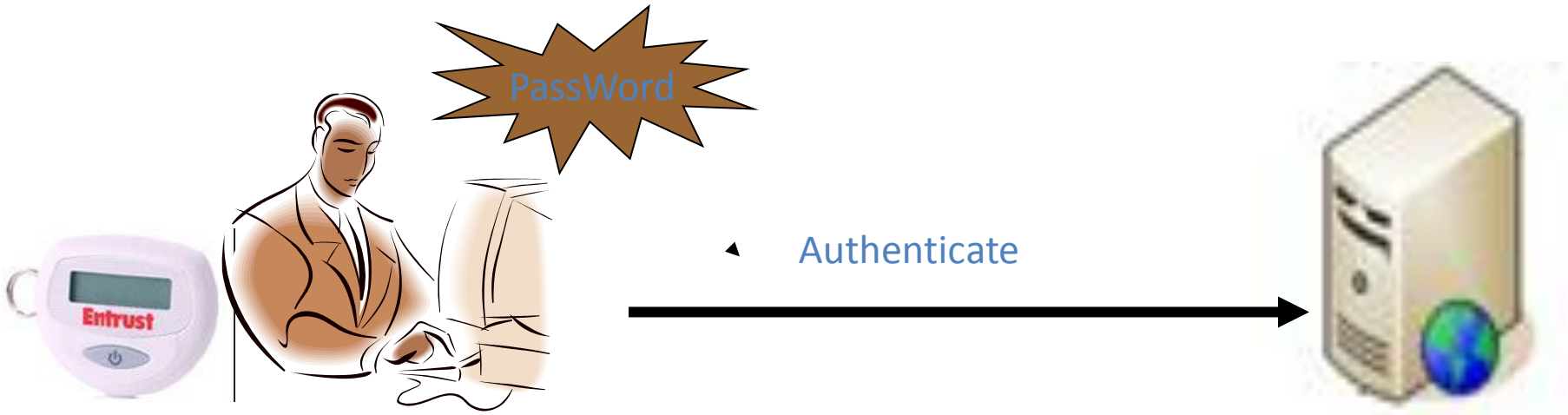
Xác thực một yếu tố

- Các hệ thống xác thực người dùng bằng Username/Password được gọi là xác thực 1 yếu tố

❖ *Username/password là xác thực yếu ??????*

Xác thực đa nhân tố

- Phương pháp xác thực sử dụng từ 2 yếu tố trở nên được gọi là xác thực mạnh
- Ví dụ xác thực 2 yếu tố là phương pháp xác thực yêu cầu 2 yếu tố phụ thuộc vào nhau để chứng minh tính đúng đắn của một danh tính dựa trên :
  - Những thông tin mà người dùng biết (số PIN, mật khẩu)
  - Cùng với những gì mà người dùng có (SmartCard, USB, Token,…)



Sử dụng mật khẩu đúng cách

- **Tại sao cần phải như vậy, tôi chỉ cần giữ kín mật khẩu là được chứ?**
  - Nếu mật khẩu là chính tên, ngày sinh của bạn hoặc gia đình: ai đó không cần công cụ cũng có thể đoán ra
  - Nếu mật khẩu dưới 4 ký tự: hacker chỉ cần vài phút để biết.
  - Nếu mật khẩu của bạn có 7 ký tự nhưng toàn là chữ: chỉ mất vài giờ đến một ngày
  - Nếu mật khẩu của bạn có ký tự và số: cần vài ngày đến hàng tuần
  - Nếu mật khẩu của bạn được đặt theo đúng cách nói trên: cần hàng năm đến hàng chục năm.

Sử dụng mật khẩu đúng cách

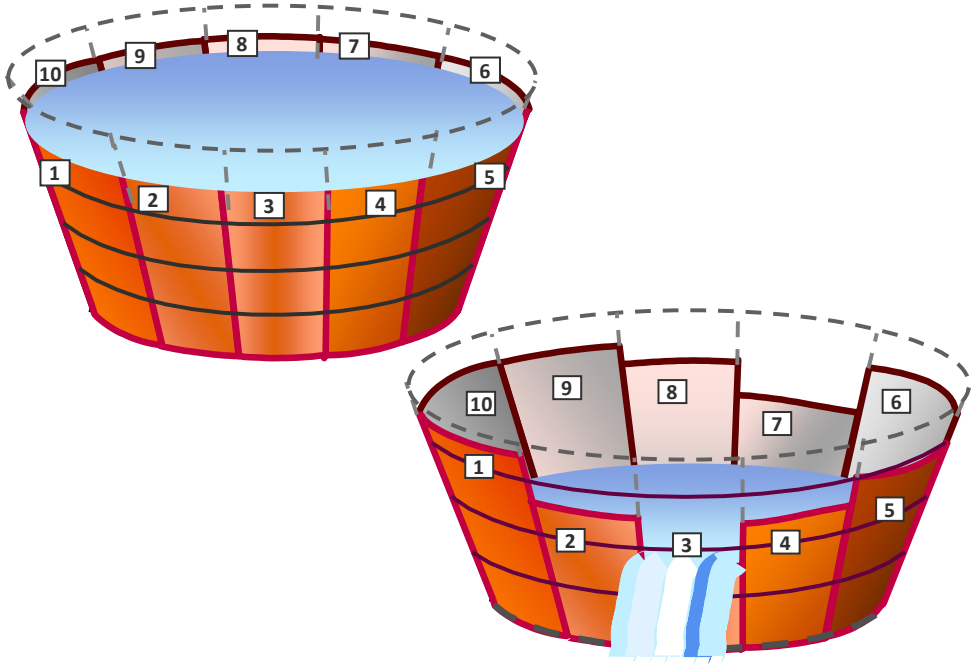
- **Hãy để cho mật khẩu đảm bảo tính bí mật, chỉ bạn biết:**
  - Khi đăng nhập đừng để người khác nhìn
  - Không viết mật khẩu ra giấy rồi dán ở nơi dễ nhìn như một tờ nhắc việc
  - Hạn chế đưa mật khẩu của mình cho người khác mượn, nếu bắt buộc phải làm, hãy nhớ đổi mật khẩu ngay sau đó
- **Làm cho mật khẩu của bạn trở nên khó đoán:**
  - Đừng đặt mật khẩu trùng với username
  - Nên đặt 7 hoặc 14 hoặc 21 ký tự với windows.
  - Đừng dùng những thông tin cá nhân của bạn để đặt mật khẩu. Ví dụ: user name là MinhHa, mật khẩu là hanm.
  - Nên có cả chữ hoa chữ thường, số và ký tự đặc biệt như $%^&!><?
- **Một số cách đặt mật khẩu để an toàn và dễ nhớ:**
  - Chuyển chữ thành số, ký tự đặc biệt có hình dạng giống: hacker =h@ck3r
  - "Mã hóa câu gợi ý mật khẩu": 1 café vào 7h sáng = 1cf@7am….

Công cụ bảo mật

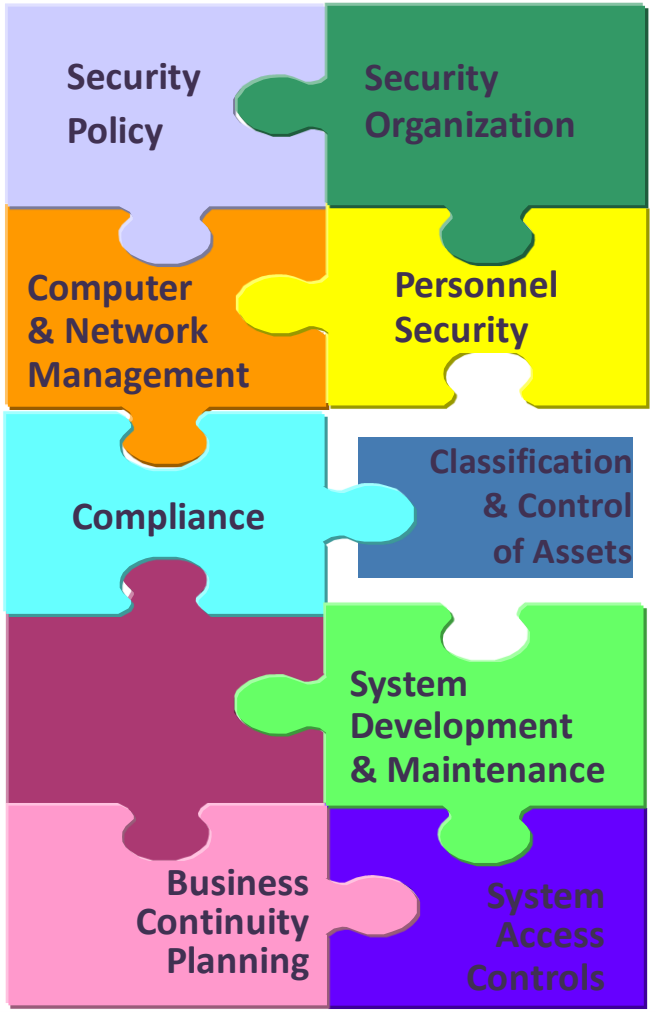
- Các công cụ bảo mật hiện nay bao gồm có cả phần cứng và phần mềm, tiêu biểu như:
  - Phần mềm diệt virus
  - Thiết bị/ phần mềm tường lửa
  - Thiết bị/ phần mềm phòng chống xâm nhập
  - Thiết bị cửa bảo vệ, camera quan sát
  - Thiết bị báo động
  - …

Tại sao lại cần phải quản lý về An toàn Thông tin?

How much is Enough?



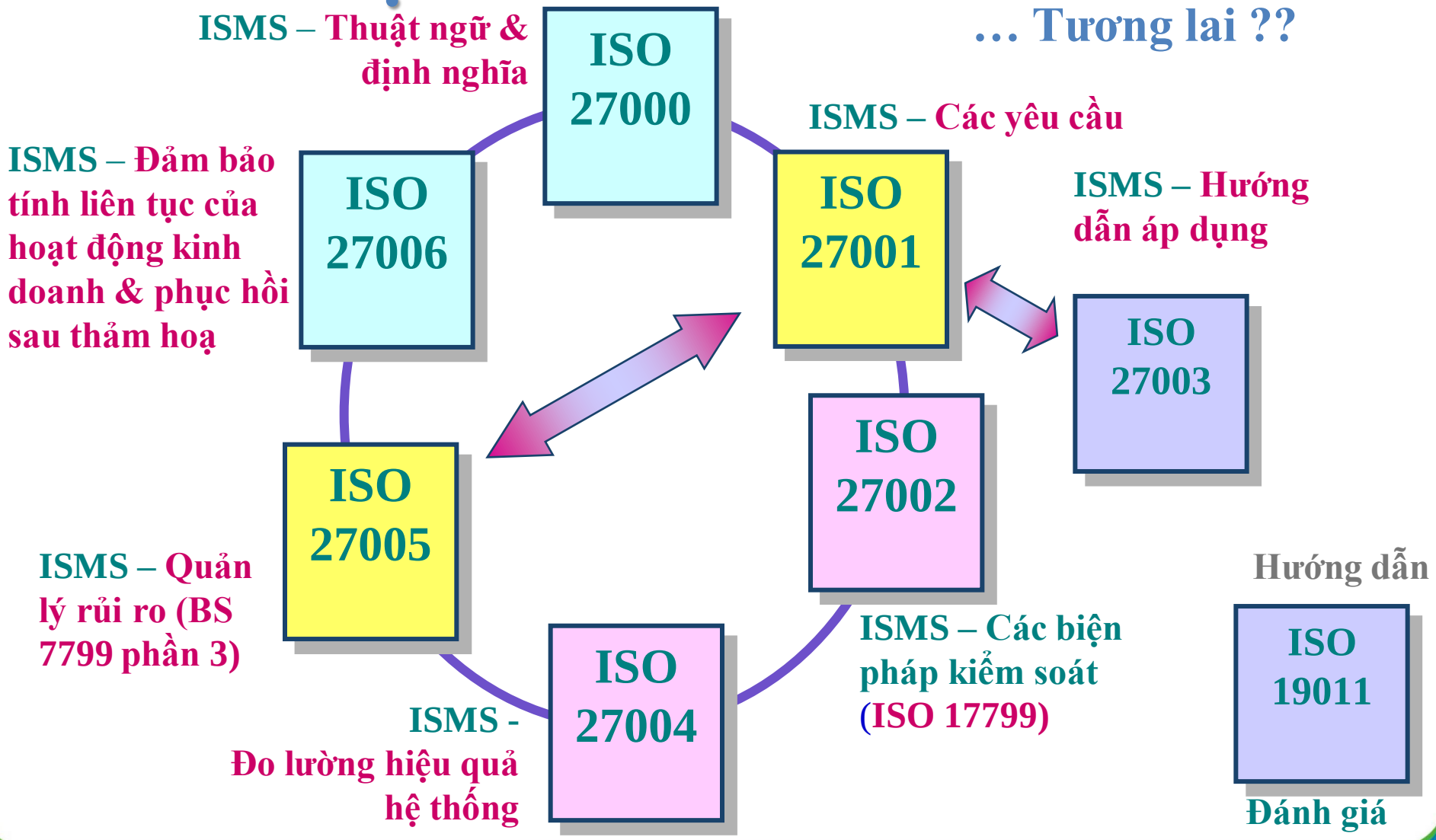
ISO 17799 (Best Practices)



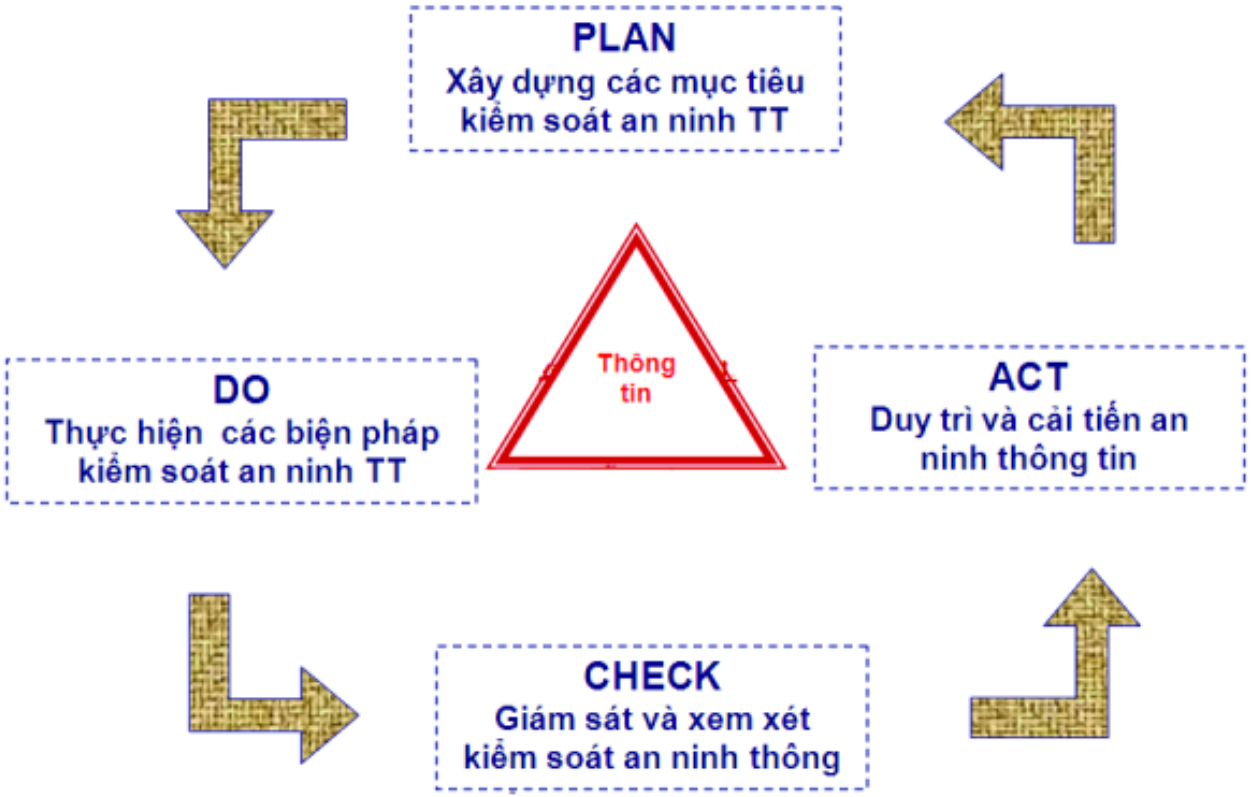
Khái niệm

- Tiêu chuẩn ISO 27001:2005 có nghĩa là :
  - Tiêu chuẩn do tổ chức ISO ban hành
  - Số thứ tự 27001
  - Ban hành năm 2005
- ISO 27001:2005
  - Chuẩn ISO 27001 là chuẩn quốc tế cung cấp mô hình để xây dựng, vận hành, quản lý, duy trì và cải tiến hệ thống BMTT.
  - Cung cấp các phương pháp kiểm soát nhằm giảm rủi ro cho tài sản của công ty tới mức thấp nhất có thể.
- **ISMS** (Information Security Management Systems): Hệ thống quản lý An toàn thông tin

Bộ tiêu chuẩn ISO 27000



PCDA


PLAN
Xây dựng các mục tiêu kiểm soát an ninh TT
DO
Thực hiện các biện pháp kiểm soát an ninh TT
Thông tin
ACT
Duy trì và cải tiến an ninh thông tin
CHECK
Giám sát và xem xét kiểm soát an ninh thông

Quá trình thiết lập và quản lý ISMS

Plan

Xây dựng hệ thống ISMS

Do

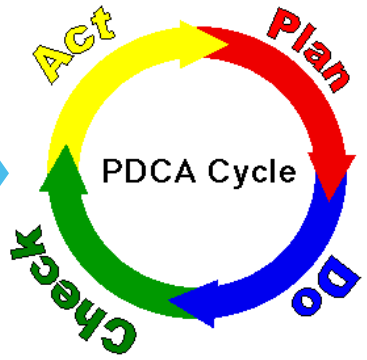
Vận hành hệ thống ISMS

Check

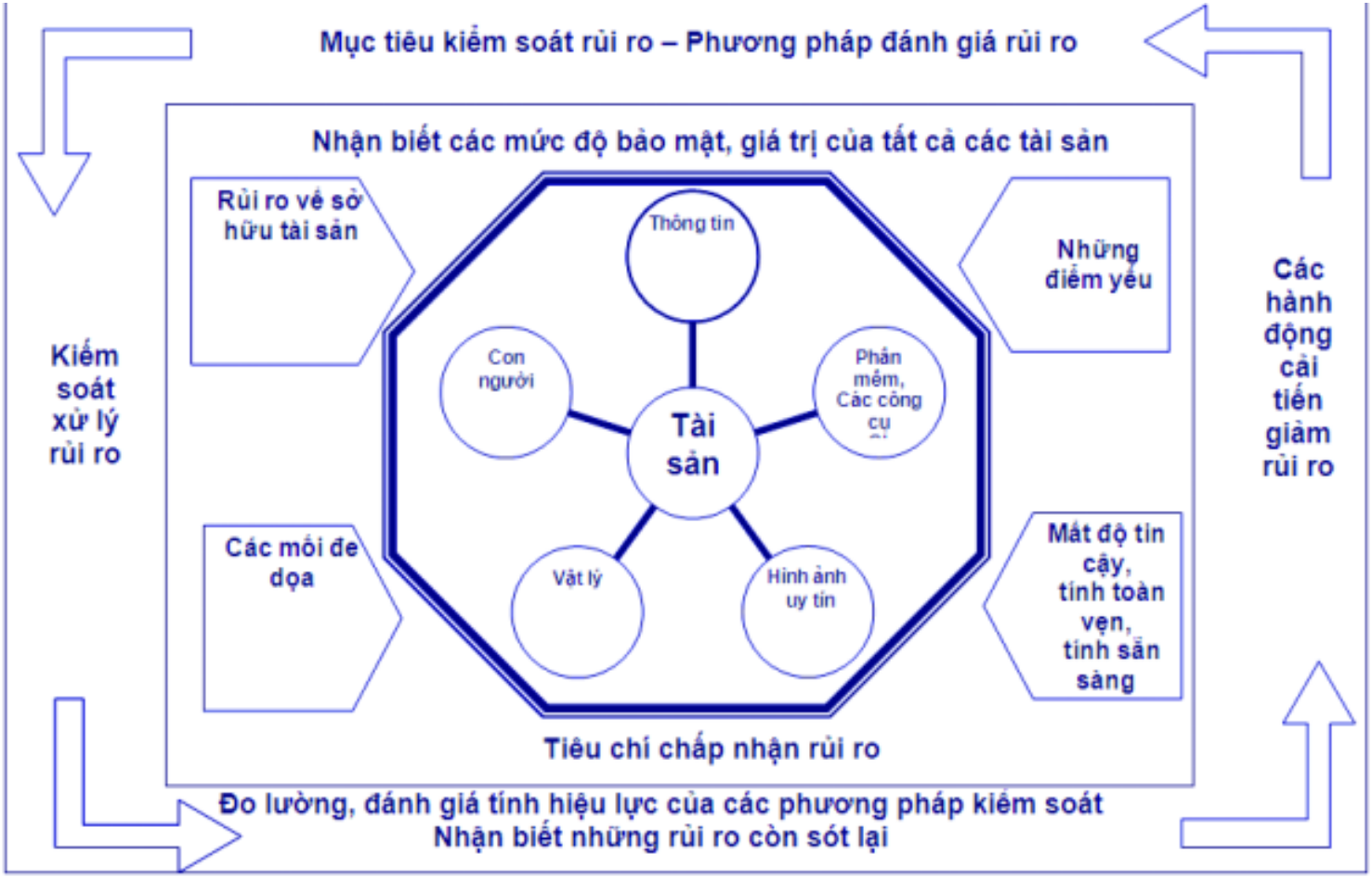
Đánh giá kiểm soát hệ thống ISMS

Act

Duy trì, cải tiến hệ thống ISMS



Tài sản


Mục tiêu kiểm soát rủi ro – Phương pháp đánh giá rủi ro
Nhận biết các mức độ bảo mật, giá trị của tất cả các tài sản
Rủi ro về sở hữu tài sản
Những điểm yếu
Thông tin
Con người
Phần mềm, Các công cụ
Tài sản
Vật lý
Hình ảnh uy tín
Các mối đe dọa
Mất độ tin cậy, tính toàn vẹn, tính sẵn sàng
Tiêu chí chấp nhận rủi ro
Đo lường, đánh giá tính hiệu lực của các phương pháp kiểm soát
Nhận biết những rủi ro còn sót lại
Kiểm soát xử lý rủi ro
Các hành động cải tiến giảm rủi ro

Các bước xây dựng

Mục tiêu

- Tính toán các mục tiêu và yêu cầu về thông tin
- Đảm bảo các rủi ro được quản lý với chi phí hiệu quả
- Tuân thủ các quy định và pháp luật
- Là phần khung cho việc triển khai và quản lý để đạt được các mục tiêu về thông tin của tổ chức.
- Giúp xác định, phân loại các tiến trình quản lý thông tin đang có của tổ chức
- Được sử dụng để xác định, phân tích các tình trạng quản lý thông tin
- Được đánh giá viên sử dụng để đánh giá mức độ phù hợp của tổ chức so với tiêu chuẩn.

10 Quy Tắc Then Chốt Trong Bảo Mật

1. Nếu một người nào đó có thể thuyết phục bạn chạy chương trình của anh ta trên máy tính của bạn, Nó sẽ không còn là máy tính của bạn nữa
2. Nếu một người nào đó có thể sửa đổi hệ điều hành trên máy tính của bạn, nó sẽ không còn là máy tính của bạn nữa
3. Nếu một người nào đó truy cập vật lí không hạn chế tới máy tính của bạn. nó sẽ không còn là máy tính của bạn nữa
4. Nếu bạn cho phép một người nào đó đẩy các chương trình tới website của bạn. Nó sẽ không còn là website của bạn
5. Các mật khẩu dễ nhận có thể làm hỏng hệ thống bảo mật mạnh
6. Một hệ thống chỉ có độ an toàn như sự tin tưởng nhà quản trị
7. Dữ liệu được mã hoá chỉ như chìa khoá giải mã
8. Một hệ thống quét virus hết hạn thì cũng còn tốt hơn không có hệ thống diệt virus nào
9. Tình trạng dấu tên hoàn toàn không thực tế
10. Công nghệ không phải là tất cả

Thank You !