

MỤC LỤC

THƯ CHÀO MỪNG	3
PHẦN 1: NỘI DUNG.....	4
CHƯƠNG TRÌNH HỘI THẢO.....	4
HIỆN TRẠNG VỀ ATTT KHU VỰC PHÍA NAM.....	6
CÔNG TÁC ĐẢM BẢO AN TOÀN AN NINH THÔNG TIN CHO CÁC CƠ QUAN NHÀ NƯỚC TRÊN ĐỊA BÀN THÀNH PHỐ	17
BÁO CÁO CỦA ORACLE.....	21
CƠ SỞ HẠ TẦNG NĂNG ĐỘNG BẢO VỆ TÀI SẢN DOANH NGHIỆP.....	35
TỔNG QUAN CISCO SAFE: KIẾN TRÚC AN NINH MẠNG THẾ HỆ MỚI ĐÃ ĐƯỢC KIỂM CHỨNG TRONG THỰC TẾ	36
HỆ THỐNG QUẢN LÝ ATTT THEO ISO 27001:2005 CÁCH TIẾP CẬN VÀ ÁP DỤNG THỰC TẾ	52
SESSION 1: ATTT MẠNG VÀ HỆ THỐNG	65
GIẢI PHÁP CHỐNG THẤT THOÁT DỮ LIỆU CHO DOANH NGHIỆP.....	66
ĐẢM BẢO TÍNH LIÊN TỤC CỦA DOANH NGHIỆP VÀ KHÔI PHỤC SAU THẢM HỌA	83
SESSION 2: ĐÀO TẠO VÀ CHUẨN HÓA TRONG ATTT	97
ĐÀO TẠO VÀ CHUẨN HÓA ATTT	98
ĐỊNH GIÁ TÀI SẢN HỆ THỐNG THÔNG TIN	105
ĐÁNH GIÁ NGUY CƠ ATTT	111
CON ĐƯỜNG TRỞ THÀNH CHUYÊN VIÊN AN NINH MẠNG.....	119
SESSION 3: ATTT TRONG THƯƠNG MẠI ĐIỆN TỬ	125
CÔNG NGHỆ XÁC THỰC HIỆN ĐẠI DỰA TRÊN SMARTCARD VÀ KẾT HỢP VỚI BIOMETRICS	126
PHÒNG TRÁNH RỦI RO CHO MÁY CHỦ WEB VỚI MICROSOFT SYSTEM CENTER	139
PHẦN 2: THÔNG TIN NHÀ TÀI TRỢ.....	153
1. Oracle	153
2. IBM Vietnam	155
3. HP.....	157
4. Cisco.....	159
5. Microsoft	163
6. BUREAU VERITAS.....	164
7. TRUSTBank.....	168
8. Secude.....	171
9. Kaspersky	174
10. Astaro	175
11. Khu CNPM Đại học quốc gia TP.HCM.....	176
PHẦN 3: THÔNG TIN ĐƠN VỊ TỔ CHỨC VÀ HỘI VIÊN	177
1. SỞ THÔNG TIN VÀ TRUYỀN THÔNG TP. HỒ CHÍ MINH	177
2. HIỆP HỘI ATTT VIỆT NAM và CHI HỘI ATTT PHÍA NAM.....	178
3. HPT.....	181
4. Misoft	184
5. Athena	186
6. Mắt Bão	188

7.	VIETPACE	189
8.	VIETUNION CORP	192
9.	NTS Group.....	194

PHỤ LỤC: BÁO CÁO CHUYÊN ĐỀ CỦA CHI HỘI NĂM 2009

THƯ CHÀO MỪNG

(TS. Nguyễn Duy Ngọc, Chủ tịch Hiệp hội VNISA)



Ngày ATTT lần thứ 2 tại Thành phố Hồ Chí Minh do sở Thông tin – Truyền thông Thành phố phối hợp với Chi hội VNISA phía Nam tổ chức là một trong những hoạt động quan trọng trong khuôn khổ sự kiện thường niên tầm quốc gia. “Ngày ATTT Việt Nam” do Hiệp hội ATTT Việt Nam (VNISA) phối hợp với Trung tâm ứng cứu khẩn cấp máy tính Việt Nam (VNCERT) tổ chức dưới sự bảo trợ của Bộ Thông tin và Truyền thông.

Ngày ATTT Việt Nam lần thứ nhất năm 2008 đã chuyển đến toàn xã hội và cộng đồng công nghệ thông tin một thông điệp mang tính kêu gọi “chung tay xây dựng một thế giới số an toàn”. Năm 2009, một năm mà nền kinh tế thế giới và khu vực chao đảo vì cơn bão suy thoái, kinh tế Việt Nam cũng vì thế mà chịu ảnh hưởng không nhỏ. Các thông tin về sự cố mất ATTT tại Việt Nam cũng xuất hiện ngày càng nhiều trên các phương tiện thông tin và truyền thông. Cũng chính vì vậy mà chủ đề của sự kiện thường niên “Ngày ATTT Việt Nam” năm nay là “Bảo vệ tài nguyên thông tin hôm nay vì ngày mai phát triển”.

Trung thành với mục đích, tôn chỉ cao cả của Hiệp hội là hướng đến việc bảo vệ ATTT cho cộng đồng doanh nghiệp và xã hội. Vì vậy sự kiện thường niên ngày ATTT Việt Nam năm nay cũng sẽ là dịp thể hiện sự gắn kết giữa nhà nước, xã hội và doanh nghiệp trong lĩnh vực ATTT. Đồng thời cũng là cơ hội để cộng đồng các doanh nghiệp, cá nhân, tổ chức tiếp cận, chia sẻ thông tin, kiến thức, kinh nghiệm; trình diễn giới thiệu những công cụ giải pháp, sản phẩm mới nhất về ATTT.

Ban Chấp hành Hiệp hội ATTT (VNISA) tin tưởng rằng: Phát huy những thắng lợi, kế thừa những kinh nghiệm quý báu của ngày ATTT Việt Nam lần thứ nhất, ngày ATTT Việt Nam lần thứ 2 tại thành phố Hồ Chí Minh năm nay cùng với chuỗi các hoạt động trong khuôn khổ sự kiện thường niên đang sôi nổi diễn ra trong cả nước sẽ được tổ chức long trọng, thiết thực, thành công và thực sự trở thành một ngày hội của cộng đồng công nghệ thông tin nói chung và những người nghiên cứu, ứng dụng, phát triển ATTT nói riêng. Thông qua đó góp phần xây dựng Hiệp hội ATTT Việt Nam ngày càng vững mạnh.

T/M Ban Chấp hành

CHỦ TỊCH HIỆP HỘI



TS. NGUYỄN DUY NGỌC

PHẦN 1: NỘI DUNG

CHƯƠNG TRÌNH HỘI THẢO

ST T	Tên chủ đề	Diễn giả	Thời gian
	Đón Khách		08h00-08h30
1	Phát biểu khai mạc	Ông Lê Mạnh Hà, Giám đốc Sở TT& TT TP. HCM	08h30-08h35
2	Tổng quan tình hình ATTT khu vực phía nam	Ông Ngô Vi Đồng, chủ tịch chi hội VNISA khu vực phía nam, tổng giám đốc công ty HPT	08h35-08h45
3	ATTT cơ sở dữ liệu	Ông Đỗ Bình, Technology Senior Solution Consultant, Oracle	08h45-09h15
4	Cơ sở hạ tầng năng động bảo vệ tài sản doanh nghiệp	Đại diện công ty IBM	09h15-09h35
5	Tổng quan Cisco SAFE: Kiến trúc an ninh mạng thế hệ mới đã được kiểm chứng trong thực tế	Ông Phan Thanh Sơn, Giám đốc Công nghệ Công ty Cisco Systems Việt nam	09h35-09h55
6	Hệ thống Quản lý ATTT (ISMS) theo ISO 27001:2005 - Cách tiếp cận & áp dụng thực tế	Ông Trịnh Tuấn Dũng, Giám đốc kiểm định công ty BVQI	09h55-10h10
7	Tọa đàm về ATTT	Diễn giả, chuyên gia ATTT	10h10-10h45
Nghỉ giải lao			10h45-11h00
Session 1: ATTT mạng và hệ thống			11h00-12h30
Người điều phối: Ông Phùng Hải, trưởng ban ATTT mạng và hệ thống, chi hội VNISA phía Nam.			
1	Giải pháp chống thất thoát dữ liệu cho doanh nghiệp	Ông Nguyễn Thành Nam, chuyên gia bảo mật công ty HPT	
2	Đảm bảo tính liên tục của doanh nghiệp và khôi phục sau thảm họa	Ông Đỗ Ngọc Huy, chuyên gia bảo mật công ty FPT	
3	Thảo luận + Bốc thăm trúng thưởng		
Session 2: Đào tạo và Chuẩn hóa trong ATTT			11h00-12h30
Người điều phối: TS. Trịnh Ngọc Minh, Khu CNPM ĐHQG-HCM			
1	Định giá tài sản hệ thống thông tin	Ông Dương Ngọc Thái, CSO –Trưởng phòng ATTT - Ngân hàng Đông Á	

2	Đánh giá nguy cơ ATTT	Ông Đặng Hoàng Minh, Senior IT Manager - GLOBAL CYBERSOFT (VN) JSC.	
3	Con đường trở thành chuyên viên an ninh mạng.	Th.S Sử Tam Nguyên, Giảng viên hệ thống Cisco (CCSI) – Saigon CTT.	
4	Thảo luận + Bốc thăm trúng thưởng		
Session 3: ATTT trong Thương Mại Điện Tử			11h00-12h30
Người điều phối: TS. Võ Văn Khang, Phó Tổng Giám Đốc Ngân Hàng Việt Á			
1	Công nghệ xác thực hiện đại	Ông Nguyễn Hữu Dũng, giám đốc công ty Secude Việt Nam	
2	Phòng tránh rủi ro cho máy chủ web với Microsoft system center.	Ông. Vũ Sơn, chuyên gia kỹ thuật Microsoft	
3	Thảo luận + Bốc thăm trúng thưởng		

HIỆN TRẠNG VỀ ATTT KHU VỰC PHÍA NAM

(Ông Ngô Vi Đồng, Chủ tịch Chi hội VNISA khu vực phía Nam, Tổng Giám Đốc công ty HPT)



Tiếp nối sự kiện ngày ATTT được tổ chức thành công vào ngày 18/11/2008, Chi hội ATTT khu vực phía Nam tổ chức ngày ATTT lần thứ 2 vào ngày 18/11/2009. Như thông lệ, trước ngày ATTT, Chi hội ATTT đã tiến hành khảo sát thực trạng ứng dụng triển khai ATTT tại các cơ quan doanh nghiệp trên địa bàn TP. HCM và các tỉnh thành thuộc khu vực phía Nam. Bản báo cáo này đi qua một số sự kiện nổi bật về tình hình ATTT trên thế giới nói chung và phân tích tình hình thực hiện ATTT tại Việt Nam nói riêng, đồng thời đề xuất một số kiến nghị về ATTT đối với các doanh nghiệp và cơ quan quản lý nhà nước.

Báo cáo bao gồm các phần chính:

1. Xu hướng về ATTT trên thế giới và Việt Nam năm 2009
2. ATTT tại Việt Nam, những cuộc tấn công và thiệt hại trong năm 2009
3. Kết quả khảo sát tình trạng ATTT tại Tp. HCM và khu vực phía Nam năm 2009 và một số nhận định đánh giá
4. Các giải pháp, công nghệ và ứng dụng ATTT hiện có tại Việt Nam
5. Nguồn nhân lực và đào tạo ATTT tại khu vực phía Nam
6. Công tác truyền thông, tuyên truyền về ATTT
7. Các quy định, luật lệ về ATTT
8. Các cơ quan quản lý nhà nước và bảo vệ pháp luật trong công tác phòng chống tội phạm công nghệ cao
9. Chi hội ATTT phía Nam và các doanh nghiệp cung cấp giải pháp, dịch vụ ATTT
10. Kết luận, kiến nghị

1. Xu hướng về ATTT trên thế giới và Việt Nam năm 2009

Năm 2009 gần đi qua với dấu ấn của sự ảnh hưởng từ cuộc khủng hoảng suy thoái toàn cầu, tác động trực diện đến hầu như tất cả các hoạt động kinh tế xã hội. Tuy nhiên, ngành ATTT được đánh giá là ngành miễn nhiễm yếu tố suy thoái. Thậm chí theo đánh giá từ một số tổ chức, chi phí đầu tư và mối quan tâm đến ATTT của một số công ty đã đi ngược chiều suy thoái và có đà gia tăng. Sở dĩ có sự lợi ngược dòng này là do đối với nhiều công ty trên thế giới, ATTT là một thành phần cốt lõi chặt chẽ không thể thiếu được cho tất cả những hoạt động kinh doanh hiện tại, cũng như cho những hoạt động cải thiện hiệu quả kinh doanh, cần thiết cho sự sống còn của công ty trong thời kỳ khủng hoảng.

Mặc dù đầu tư và chi phí cho ngành ATTT tiếp tục gia tăng, các cuộc tấn công ATTT vẫn liên tục xảy ra và ngày càng phức tạp tinh xảo hơn. Điển hình là sự kiện hacker ăn cắp hàng triệu thẻ tín dụng từ các công ty tài chính, thanh toán điện tử vào tháng 1 năm 2009. Về phía người dùng, trong năm 2009 đã xuất hiện liên tục các mã độc malware mới lợi dụng các lỗ hổng của hệ điều hành và ứng dụng để tấn công ăn cắp dữ liệu, gửi spam... Tiếp đó phải kể đến sự cố tấn công từ chối dịch vụ vào các trang Web chính phủ của Mỹ và Hàn Quốc vào tháng 7/2009. Điều này cho thấy vấn đề ATTT đã trở thành mối nguy cơ đe dọa an ninh của mỗi quốc gia.

Theo các chuyên gia, xu hướng ATTT năm 2009 có thể kể đến:

- ATTT cho máy trạm (end point security) tiếp tục là điểm nóng. Với sự đa dạng hóa của các thiết bị đầu cuối (máy tính để bàn, điện thoại thông minh, laptop, netbook...) dẫn đến nguy cơ hacker tấn công trực tiếp vào máy người dùng để ăn cắp dữ liệu bằng các phần mềm mã độc malware. Ở mặt trận phòng thủ, các giải pháp chống virus truyền thống đã dần tiến hóa kết hợp nhiều chức năng như chống virus, spyware, spam, malware, tường lửa, mã hóa ổ cứng, chống thất thoát dữ liệu.

- ATTT cho các lĩnh vực mới như điện toán đám mây, ảo hóa. Đây là những xu hướng mới của ngành CNTT và ATTT tiếp tục là mối quan tâm hàng đầu của các công ty khi triển khai các dịch vụ trên.
- Với sự gia tăng cấp số nhân về số lượng người sử dụng, mạng xã hội tiếp tục trở thành tiêu điểm của các cuộc tấn công ATTT. Điển hình là các cuộc tấn công vào các trang mạng xã hội phổ biến như twitter, myspace, facebook gần đây.
- ATTT trong các thiết bị di động. Là hệ quả tất yếu của sự bùng nổ các thiết bị di động thông minh có chức năng như một máy tính độc lập. Các tấn công vào thiết bị di động đang có chiều hướng ngày càng gia tăng.
- Xu hướng tấn công Web lợi dụng các lỗ hổng Web truyền thống, cũng như các lỗ hổng Web 2.0. Đã xuất hiện những cuộc tấn công Web nghiêm trọng lợi dụng những lỗ hổng Web tưởng chừng như đã lỗi thời như tấn công SQL injection gây hậu quả mất cắp hàng triệu thẻ tín dụng tại một công ty tài chính.
- Tấn công nội mạng xuất phát từ các nhân viên nội bộ vẫn tiếp tục gia tăng và là một trong những mảng cần sự quan tâm đặc biệt trong chiến lược xây dựng ATTT tổng thể.
- Sự gia tăng các nỗ lực phối hợp đa quốc gia trong mặt trận phòng chống tội phạm an ninh mạng. ATTT ngày nay đã trở thành vấn đề toàn cầu và cần sự cộng tác phối hợp giữa các tổ chức có thẩm quyền từ mỗi quốc gia để có thể giải quyết triệt để.

Bảo vệ thông tin ngày nay chính là bảo vệ tài sản cá nhân, tài sản doanh nghiệp, tài sản quốc gia và cao hơn cả là bảo vệ tài sản của nhân loại.

2. ATTT tại Việt Nam, những cuộc tấn công và thiệt hại trong năm 2009

Ở Việt Nam, sự kiện Việt Nam đứng đầu danh sách các nước giả mạo click do tổ chức Anchor Intelligence công bố đã gióng lên hồi chuông cảnh báo. Điều này cho thấy tình hình ATTT tại Việt Nam vẫn còn yếu kém và đã ảnh hưởng rất lớn đến nền kinh tế, cũng như hình ảnh và uy tín của Quốc gia trong lĩnh vực thương mại điện tử. ATTT đã trở thành yếu tố sống còn để bảo vệ sự phát triển bền vững ngày mai của nền kinh tế ngày càng phụ thuộc vào thông tin. Đây cũng là thông điệp mà ngày hội ATTT năm 2009 với chủ đề “Bảo vệ tài nguyên thông tin hôm nay vì ngày mai phát triển” muốn gửi gắm.

Tình hình ứng dụng ATTT tại Việt Nam vẫn chưa thực sự đủ mạnh để có thể ngăn ngừa và chống lại các cuộc tấn công. Đã có nhiều Website của tổ chức, doanh nghiệp và thậm chí của các cơ quan quản lý nhà nước bị xâm nhập để hacker cài đặt mã độc và nằm trong danh sách đen cảnh báo truy cập của Google, Websense.

Trong năm 2009, đã xuất hiện nhiều sự cố ATTT liên quan đến môi trường điện thoại di động. Với số lượng hơn 100 triệu thuê bao và sự tăng trưởng mạnh mẽ về số lượng các điện thoại thông minh, bảo mật trên điện thoại di động đã trở thành chủ đề nóng tại Việt Nam. Đã xuất hiện các cuộc tấn công giả mạo tin nhắn SMS, cài mã độc, phần mềm gián điệp trên máy điện thoại di động.

Với sự phát triển mạnh mẽ của dịch vụ giao dịch trực tuyến, đặc biệt là trong mảng chứng khoán, ngân hàng, chúng ta đang đứng trước nguy cơ tấn công từ các tin tặc có mục tiêu trục lợi rõ ràng. Trong năm 2009 đã xuất hiện một số sự kiện hacker tấn công trực lợi vào dịch vụ trực tuyến bị phát hiện và xử lý bởi cơ quan quản lý pháp luật. Điều này cho thấy sự gia tăng về mức độ tinh vi và phức tạp của các cuộc tấn công. Hacker hiện nay không đơn thuần chỉ tấn công nhằm mục đích nổi tiếng cá nhân mà có mục tiêu trục lợi rõ ràng.

3. Kết quả khảo sát tình trạng ATTT và một số nhận định đánh giá

Phương pháp khảo sát

Theo thông lệ hàng năm, trước ngày ATTT, Hiệp hội ATTT VNISA tiến hành khảo sát tình trạng ATTT dựa trên một bản câu hỏi thăm dò về ATTT gửi cho các doanh nghiệp, cơ quan có triển khai ứng dụng CNTT. Bản câu hỏi được xây dựng trên những yêu cầu về chuẩn hóa về ATTT, có tham khảo cách thức điều tra thăm dò của các tổ chức chuyên nghiệp về ATTT quốc tế.

Mục đích của cuộc điều tra thăm dò là hướng đến kết quả phản ánh nhận thức của người sử dụng CNTT về ATTT. Chúng tôi không đặt mục tiêu đưa ra những con số tuyệt đối song những dữ liệu thu thập được phần nào nói lên bức tranh về mức độ triển khai các ứng dụng ATTT và nhận thức về ATTT của các đơn vị tham gia khảo sát. Trong quá trình đi khảo sát, các chuyên gia ATTT của các thành viên chi hội ATTT phía Nam đã tích cực tiếp cận và trao đổi trực tiếp với nhiều doanh nghiệp hoạt động tại TP. HCM và một số tỉnh phía Nam. Trong số gần 1000 phiếu điều tra phát ra chỉ có hơn 200 doanh nghiệp tham gia trả lời các câu hỏi điều tra.

Sau đây là kết quả điều tra:

Đối tượng khảo sát:

Đối tượng khảo sát chủ yếu là các doanh nghiệp tại khu vực phía Nam, đang ứng dụng CNTT vào các hoạt động sản xuất kinh doanh. Đối tượng được phỏng vấn là các Giám Đốc CNTT (CIO), cán bộ quản lý hệ thống ATTT, chuyên gia quản trị mạng.

Phân loại các tổ chức doanh nghiệp được khảo sát:

Loại doanh nghiệp	Tỉ lệ
Tổ chức Hành chính sự nghiệp trực thuộc Trung ương	8.2 %
Tổ chức Hành chính sự nghiệp trực thuộc địa phương	11.6%
Doanh nghiệp nhà nước	9.5%
Doanh nghiệp ngoài quốc doanh	22.4%
Doanh nghiệp nước ngoài, liên doanh, có vốn nước ngoài	14.7%
Tổ chức phi chính phủ	1.7%
Khác	31.9%

Hiện trạng kết nối mạng:

- 42% doanh nghiệp được khảo sát đã có hệ thống mạng tổng thể, bao gồm kết nối LAN, WAN, và đường truyền Internet. Con số này tương đương với kết quả khảo sát năm 2008.
- 72% doanh nghiệp có mạng không dây (so với 57% năm 2008), trong đó có 48% doanh nghiệp chỉ sử dụng mạng không dây cho nhân viên nội bộ và có 24% doanh nghiệp dùng chung mạng không dây cho nhân viên và khách. Tỉ lệ này năm 2008 là 45% - 12%.
- 87% doanh nghiệp sử dụng máy chủ Windows Server, chỉ có 8.2% doanh nghiệp được khảo sát sử dụng máy chủ Linux. Các con số thống kê năm 2008 là 83% - 10%.

Mức độ sẵn sàng:

- 47% doanh nghiệp đã gán trách nhiệm ATTT đến nhân viên chuyên trách (58% - 2008)
- 100% doanh nghiệp đã có sử dụng phần mềm Anti-Virus (20% - 2008)
- Chỉ có 10% doanh nghiệp được khảo sát không sử dụng tường lửa firewall (40% - 2008)
- 50% doanh nghiệp hiện không có quy trình xử lý sự cố ATTT (70% - 2008)
- 74% doanh nghiệp được hỏi hiện không có chính sách ATTT (85% - 2008)
- 59% doanh nghiệp dự tính sẽ tăng ngân sách đầu tư ATTT (74% - 2008)
- 35% doanh nghiệp đưa ra mức tỉ lệ đầu tư an ninh mạng trong tổng ngân sách CNTT là 5%, 26% doanh nghiệp đưa ra mức 5%-10% (36% - 32% năm 2008)
- 50% doanh nghiệp hiện không có quỹ dự phòng cho các rủi ro an ninh mạng

Phát hiện và xử lý tấn công an ninh mạng

Tính từ tháng 1/2009:

- 34% doanh nghiệp thừa nhận đã phát hiện sự cố tấn công an ninh mạng (28% năm 2008)
- 38% doanh nghiệp không hề biết rõ hệ thống mạng của mình có bị tấn công hay không (26% năm 2008)
- Trong các tấn công an ninh mạng phát hiện được: 43% các tấn công do Virus, 65% là do mã độc hại và sâu Internet (40%, 60% - 2008).
- 25% doanh nghiệp được hỏi phản hồi là không hiểu rõ được động cơ đằng sau các cuộc tấn công an ninh mạng. (25% - 2008).
- 45% doanh nghiệp không có hệ thống an ninh mạng có khả năng ghi nhận được các tấn công (55% - 2008).
- 68% doanh nghiệp không thể ước lượng được mức độ thiệt hại của các tấn công an ninh mạng. (67% - 2008)
- 53% doanh nghiệp ước tính mức độ thiệt hại lớn nhất của các sự cố an ninh mạng là do Virus (80% - 2008)

Xử lý và tường thuật sự cố

- Chỉ có 10% doanh nghiệp sẵn sàng báo cho cơ quan pháp luật khi có sự cố an ninh mạng (5% - 2008)
- 60% doanh nghiệp trả lời lý do chính của việc e ngại liên lạc với cơ quan pháp luật là do tâm lý sợ ảnh hưởng đến hình ảnh doanh nghiệp (50% - 2008)

Nhận xét

Qua kết quả thu được từ cuộc khảo sát, chúng tôi nhận thấy:

- Vấn đề nhận thức về ATTT chưa được quan tâm đúng mức. Kết quả thống kê cho thấy 80% các sự cố về ATTT do yếu tố con người nhưng thật đáng tiếc không có thống kê nào cho thấy việc đầu tư nâng cao nhận thức cho nhân viên về ATTT trong doanh nghiệp được chú trọng thực hiện.
- Tình trạng ATTT tại các doanh nghiệp phía Nam hiện đang ở mức dưới trung bình do thực trạng đầu tư vào hệ thống phòng thủ an ninh mạng còn rất yếu. Tuy nhiên đã có dấu hiệu khả quan cho thấy mức độ nhận thức ATTT tại các doanh nghiệp đang tăng dần đi đôi với việc dự báo tăng ngân sách cho các dự án ATTT.
- Tỷ lệ doanh nghiệp đã xây dựng chính sách ATTT ở mức thấp, điều này thể hiện sự thiếu kiến thức của doanh nghiệp về việc xây dựng hệ thống ATTT tổng thể. Đi đôi với sự thiếu vắng của việc cam kết xây dựng hệ thống ATTT từ các cấp lãnh đạo.
- Các doanh nghiệp hiện chỉ chú trọng đầu tư vào thiết bị và phần mềm bảo mật, rất ít doanh nghiệp hiểu được tầm quan trọng của việc xây dựng quy trình ATTT, hệ thống quản lý ATTT tổng thể theo chuẩn ISO-17799.
- Tỷ lệ doanh nghiệp có hệ thống anti-virus có bản quyền còn thấp mặc dù theo thống kê thì gần 100% doanh nghiệp đã dùng phần mềm anti-virus. Đa số các doanh nghiệp vẫn sử dụng hệ thống anti-virus không có bản quyền hợp pháp.
- Phần lớn các sự cố an ninh mạng phát hiện được đều liên quan đến các sự cố anti-virus và web. Là những sự cố có thể được phát hiện dễ dàng. Có thể còn tiềm ẩn những tấn công nội mạng mà doanh nghiệp hiện chưa quan tâm đúng mức. Vì lý do nhạy cảm, rất khó thống kê được số lượng thực tế các tấn công nội mạng này. Đây là mối nguy cơ tiềm ẩn rất đáng quan tâm.
- Doanh nghiệp đang gặp nhiều khó khăn trong vấn đề phát hiện và xử lý sự cố ATTT. Nguyên nhân chính là việc thiếu đầu tư các thiết bị có khả năng phát hiện, ghi nhận sự cố ATTT. Đi đôi với sự thiếu vắng của các quy trình thủ tục xử lý sự cố, và tâm lý e ngại liên hệ với cơ quan luật pháp.

- Thiếu trầm trọng nguồn nhân lực bảo mật cho tổ chức và doanh nghiệp. Rất ít tổ chức có nhân viên quản trị bảo mật thông tin chuyên trách hay giám đốc, trưởng phòng bảo mật (Security manager).
- Công tác đào tạo nguồn nhân lực ATTT chưa được các tổ chức, doanh nghiệp đánh giá đúng mức.

4. Các giải pháp, công nghệ và ứng dụng ATTT hiện có tại Việt Nam

Hiện nay trên thị trường Việt Nam đã ứng dụng nhiều giải pháp ATTT từ nhiều hãng bảo mật quốc tế có tên tuổi lẫn các nhà cung cấp nội địa. Dưới đây là một số giải pháp và công nghệ nổi bật:

Phân Loại	Chức Năng	Nhà sản xuất và công ty phân phối tại Việt Nam
End Point Security (anti-virus)	Phòng chống Virus	Trend Micro(Misoft). Kaspersky (NTS), McAfee (Mi2), Symantec (FPT, Ingram Micro), BKAV, Bitdefender (VIAMI), Kingsoft Anti-Virus (Quang Minh DEC), Sophos (MTech)
End Point Security multi-vector: anti-virus, anti-malware, anti-spam, url-filtering)	Phòng chống các tấn công do mã độc	Trend Micro(Misoft). Kaspersky (NTS), McAfee (Mi2), Symantec (FPT, Ingram Micro).
End Point Security: Mã hóa dữ liệu	Mã hóa dữ liệu ổ cứng.	Check Point (Misoft) Entrust (Misoft) PGP (MTech)
End Point Security: Chống thất thoát dữ liệu	Phòng ngừa các nguy cơ thất thoát dữ liệu ở máy trạm	Check Point (Misoft) McAfee (Mi2) Trend Micro (Misoft) Patchlink Lumension (MTech)
End Point Security: Kiểm soát mạng NAC	Kiểm soát truy cập mạng bằng xác thực lớp 2.	Cisco (Cisco Vietnam) Symantec (Symantec Vietnam) Juniper (J-Protect)
Phòng chống thất thoát dữ liệu (DLP)	Chống thất thoát dữ liệu qua các giao thức mạng.	Websense (Misoft) Symantec (Symantec Vietnam)
Tường lửa/ mạng riêng ảo Enterprise	Phòng chống các tấn công mạng và hệ thống cho môi trường Enterprise	Check Point (Misoft) Cisco (Cisco Vietnam) Juniper (J-Protect)
Tường lửa mạng UTM	Phòng chống các rủi ro dành cho doanh nghiệp SMB	Check Point (Misoft) Cisco (Cisco Vietnam) Juniper (J-Protect)

		Fortinet (M-Tech) Cyberoam (InNet) Astaro (NTS)
Hệ thống phòng chống Virus ở Gateway (Network Virus Wall)	Lọc virus, mã độc và ngăn ngừa lây lan giữa các vùng mạng.	Trend Micro (Misoft) Mcafee (Mi2)
Tường lửa chuyên dụng Web	Phòng chống các tấn công tầng Web	Barracuda (Misoft) Imperva (Misoft)
Tường lửa chuyên dụng database	Phòng chống các tấn công cơ sở dữ liệu	Imperva (Misoft)
Hệ thống phát hiện và phòng chống xâm nhập IDS/IPS	Phát hiện và phòng chống các nguy cơ xâm nhập hệ thống	IBM ISS (Misoft) Tipping Point (MTech) SourceFire (NTS) Mcafee (Mi2)
Hệ thống phát hiện và phòng chống xâm nhập IPS mạng không dây	Phát hiện và phòng chống các tấn công trên môi trường không	AirDefense (Misoft) AirTight (Misoft)
Lọc Web	Phòng chống truy cập vào các trang Web độc hại	Websense (Misoft) Trend Micro (Misoft) BlueCoat (MTech)
Chống thư rác và các hiểm họa ATTT do email	Lọc thư rác và các mã độc trên môi trường email	Barracuda (Đồng Quân) Trend Micro (Misoft) PineApp (Misoft)
Hệ thống xác thực mạnh đa thành phần	Xác thực mạnh dùng token	Entrust (Misoft) Vasco (Misoft) Verisign (Blitz) RSA (MTech) Todos (MK Technology)
Chứng chỉ số	Cung cấp chứng chỉ xác thực SSL cho máy chủ Web	Verisign (Blitz) Entrust (Misoft)
Hệ thống quản lý mật khẩu nhạy cảm Enterprise	Quản lý các tài khoản xác thực nhạy cảm trong ứng dụng và hệ thống.	Cyber-Ark (Misoft)

Đánh giá và quản lý lỗ hổng bảo mật	Dò tìm lỗ hổng bảo mật	Mcafee Foundstone (Mi2) IBM ISS (Misoft)
Quản lý log hệ thống ATTT	Theo dõi và phân tích log từ các thiết bị ATTT	ARCSight (Misoft)
Công cụ điều tra bảo mật	Thu thập bằng chứng, giám sát hoạt động mạng phục vụ cho công việc điều tra bảo mật	Encase (Misoft) AccessData (Misoft)
Công cụ làm chính sách ATTT	Giúp doanh nghiệp xây dựng chính sách ATTT	Neupart (Misoft)
Đào tạo ATTT	Cung cấp các khóa học ATTT	VietShield Misoft SaigonCTT Athena

5. Nguồn nhân lực và đào tạo ATTT tại khu vực phía Nam

- Nguồn nhân lực bảo mật thông tin có trình độ cao vẫn trong tình trạng cung không đủ cầu. Đa số các nhận sự chịu trách nhiệm đảm bảo ATTT trong doanh nghiệp là quản trị hệ thống kiêm nhiệm, phần lớn tự đào tạo, tích lũy kinh nghiệm và không được đào tạo chính quy về ATTT. Hiện vẫn có rất ít các tổ chức, doanh nghiệp tại Việt Nam có vị trí Giám đốc ATTT (CSO).
- Về đào tạo ATTT nhìn chung còn sơ khai, tự phát. Các khóa học chưa đủ để thành một chương trình đào tạo chuyên gia hoàn thiện. Các cơ sở đào tạo chủ yếu sử dụng các chương trình sẵn có của nước ngoài để giảng dạy, thiếu tính chuyên sâu và chủ yếu dạy về kỹ năng, sử dụng công nghệ "Hacking". Tại Việt Nam vẫn chưa có một bộ giáo trình chuẩn về ATTT.
- Một số cơ sở đào tạo đã có chương trình dạy về ATTT song còn ít và giáo trình cũng chưa được chuẩn hóa. Những năm gần đây đã có nhiều chuyển biến rõ rệt: số lượng người học và số lượng các môn học đều tăng, các khóa học nền tảng đã được triển khai: CCSP, SCNP, Security+, ISO 17799, CEH... Tuy nhiên đây mới chỉ là các khóa học theo chứng chỉ do các tổ chức nước ngoài cấp. Mặt khác, một bộ phận lớn học viên đăng ký các khóa học bảo mật nhằm mục đích bổ sung những chứng chỉ, bằng cấp quốc tế có tính phổ dụng chứ chưa có thái độ học tập, nghiên cứu một cách nghiêm túc để nâng cao kiến thức.
- Hệ thống đào tạo còn thiếu chương trình cho chuyên gia CISSP, CCIE security; các khóa học của InfoSec Institute về xâm nhập thử nghiệm, lập trình an toàn.
- Vấn đề đào tạo nguồn nhân lực về ATTT còn chưa được các Doanh nghiệp quan tâm đúng mức. Kiến thức về ATTT trong giới chủ doanh nghiệp còn yếu. Theo khảo sát của Ban CNTT với trên 1.200 doanh nghiệp thuộc Câu lạc bộ Doanh nhân Sài Gòn, thì có tới 90% chủ doanh nghiệp chưa ý thức được việc bảo vệ tài sản thông tin quý giá.
- Xã hội vẫn chưa đánh giá nghiêm túc sự hi sinh thầm lặng của các "chiến sĩ" quản trị và an ninh mạng. Chính đội ngũ này mới đảm bảo được hệ thống thông tin ổn định, góp phần đảm bảo hoạt động kinh doanh của doanh nghiệp.

6. Công tác truyền thông, tuyên truyền về ATTT

Các vấn đề về ATTT được đề cập đến hầu hết trong các ấn phẩm liên quan đến CNTT-TT như tạp chí Thế Giới Vi Tính – PC World VN, Tin Học và Đời Sống, Echip, Xã hội thông tin, đặc biệt là tạp chí

ATTT và chuyên mục ATTT trên Thế Giới Vi Tính Series B. Thêm vào đó, các chương trình truyền hình như “Cuộc sống số” của VTV, “1001” của HTV cũng cung cấp nhiều thông tin về ATTT.

Tuy nhiên ở mức chuyên sâu hơn phải kể đến các website, diễn đàn của giới tin học hay giới ATTT, nhất là những website có uy tín của các công ty, tổ chức chuyên về ATTT. Chẳng hạn như:

- Báo điện tử VietnamNet
- Báo điện tử VnExpress
- Chuyên mục “Bảo mật” của ICT News
- Website bảo mật thông tin
- Diễn đàn tin học, mục Bảo mật trong Tutorial room
- Tiểu mục Bảo mật trong mục Công nghệ trên VnMedia
- Website VnSecurity
- Website VietShield
- Mạng ATTT VSEC
- Diễn đàn HVAOnline
- Blog ThaiDN
- Website Athena

7. Các quy định, luật lệ về ATTT

Trong những năm qua nhà nước rất quan tâm về vấn đề ATTT. Nhiều quy định về luật pháp đã được ban hành. Các cơ quan quản lý nhà nước đã được thành lập để tập trung quản lý trong lĩnh vực ATTT và bước đầu đã phát huy được hiệu quả. Chúng ta có thể liệt kê một số điều khoản trong các bộ luật quy định những chế tài đối với các hành vi vi phạm ATTT như sau:

- Pháp lệnh Số 30/2000/PL-UBTVQH10 ngày 28/12/2000 v/v Bảo vệ bí mật Nhà nước
- Nghị định của Chính Phủ số: 33/2002/NĐ-CP Quy định chi tiết thi hành Pháp lệnh Bảo vệ bí mật nhà nước
- Bộ luật hình sự nước CHXHCNVN: điều 125, 131, 224, 225 và 226
- Bộ luật dân sự nước CHXHCNVN: Điều 31,38
- Bộ luật lao động nước CHXHCNVN: Điều 85, về hình thức xử lý kỷ luật, sa thải.
- Luật sở hữu trí tuệ Việt Nam: Điều 131.
- Luật Bảo vệ riêng tư và thông tin cá nhân
- Danh mục tài liệu bảo mật theo nghị định 123 -2002/QĐ TTg của Thủ tướng Chính phủ
- Quyết định 55/2008/BLĐTBXH để ban hành chương trình khung trình độ trung cấp nghề và cao đẳng nghề lập trình máy tính

Ngoài một số các điều khoản đã nêu ở trên, nhà nước ban hành một loạt các nghị định quy định nhiệm vụ chức năng cũng như phạm vi điều chỉnh của các cơ quan quản lý nhà nước về ATTT. Theo đó nhà nước sẽ thống nhất quản lý về ATTT thông qua các cơ quan chức năng, có thể liệt kê một số văn bản về ATTT dưới đây:

Nghị định 97/2008/NĐ-CP về quản lý, cung cấp, sử dụng dịch vụ Internet và thông tin điện tử.

Theo nghị định, các hành vi sử dụng Internet vào những mục đích sau sẽ bị cấm: Chống lại nhà nước CHXHCN Việt Nam; gây phương hại đến an ninh quốc gia, trật tự an toàn xã hội; phá hoại khối đoàn kết toàn dân... đánh cắp và sử dụng trái phép mật khẩu, khoá mã và thông tin riêng của tổ chức, cá nhân; tạo ra và cài đặt các chương trình virus máy tính, phần mềm gây hại để thực hiện một trong những hành vi quy định tại điều 71, luật CNTT.

Nghị định 90/2008/NĐ-CP về chống thư rác nghiêm cấm việc tạo điều kiện, cho phép sử dụng phương tiện điện tử thuộc quyền của mình để gửi, chuyển tiếp thư rác; trao đổi mua bán hoặc phát tán các phần mềm thu thập địa chỉ điện tử hoặc quyền sử dụng các phần mềm thu thập địa chỉ điện tử; sử dụng các phần mềm để thu thập địa chỉ điện tử khi không được phép của người sở hữu địa chỉ điện tử đó; trao đổi, mua bán danh sách địa chỉ điện tử hoặc quyền sử dụng danh sách địa chỉ điện tử nhằm mục đích gửi thư rác.

Nghị định 48/2008/NĐ-CP về quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Bộ Nội vụ: Thống nhất quản lý, bảo đảm kỹ thuật và chuyên môn nghiệp vụ cơ yếu trong phạm vi cả

nước; chủ trì, phối hợp với các Bộ, ngành trong việc thực hiện các chủ trương, chính sách của Đảng, Nhà nước liên quan đến bảo đảm an toàn và bảo mật thông tin bí mật nhà nước theo quy định của pháp luật. Giúp Chính phủ thống nhất quản lý nhà nước về mật mã dân sự, cung cấp các thiết bị và sản phẩm mật mã đáp ứng yêu cầu phát triển kinh tế, xã hội cho các tổ chức và cá nhân có nhu cầu sử dụng.

Nghị định số 64/2007/NĐ-CP về ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước, đảm bảo ATTT trên môi trường mạng. Ban Cơ yếu Chính phủ xây dựng và đề xuất ban hành các văn bản quy phạm pháp luật, tiêu chuẩn và quy chuẩn kỹ thuật, triển khai về mật mã trong an toàn và bảo mật thông tin của cơ quan Nhà nước, tổ chức kiểm định, đánh giá và cấp chứng nhận các sản phẩm mật mã trong hoạt động của cơ quan Nhà nước. Bộ Công An chịu trách nhiệm bảo đảm an ninh trong hoạt động ứng dụng công nghệ thông tin; điều tra và xử lý tội phạm trong lĩnh vực công nghệ thông tin.

Nghị định của Chính phủ số 26/2007/NĐ-CP ngày 15 tháng 02 năm 2007 quy định chi tiết thi hành luật giao dịch điện tử về chữ ký số và dịch vụ chứng thực chữ ký số. Quy định nguyên tắc giao dịch điện tử trong hoạt động tài chính; trách nhiệm, quyền hạn của tổ chức, cá nhân; trách nhiệm của các Bộ, ngành, địa phương; giải quyết tranh chấp; thanh tra, kiểm tra; xử lý vi phạm... Cơ quan tài chính và tổ chức, cá nhân có tham gia giao dịch điện tử trong hoạt động tài chính với cơ quan tài chính phải sử dụng chữ ký số; giao dịch điện tử trong hoạt động tài chính giữa tổ chức, cá nhân với cơ quan tài chính phải sử dụng chữ ký số và chứng thư số do Tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng cung cấp. Đồng thời, quy định việc thành lập, tổ chức, hoạt động và quản lý Tổ chức cung cấp dịch vụ chứng thực chữ ký số chuyên dùng phục vụ cho các giao dịch điện tử trong hoạt động tài chính của cơ quan tài chính.

Nghị định số 73/2007/NĐ-CP về hoạt động nghiên cứu, sản xuất, kinh doanh và sử dụng mật mã để bảo vệ thông tin không thuộc phạm vi bí mật nhà nước. Danh mục sản phẩm mật mã dân sự (MMDS) phải áp dụng Quy chuẩn kỹ thuật quốc gia trong từng thời kỳ do Ban Cơ yếu Chính phủ chủ trì, phối hợp với Bộ Khoa học và Công nghệ xây dựng, trình cơ quan có thẩm quyền ban hành. Danh mục này được rà soát hằng năm để bổ sung các sản phẩm mật mã dân sự bắt buộc phải áp dụng Quy chuẩn kỹ thuật quốc gia theo quy định hiện hành.

8. Các cơ quan quản lý nhà nước và bảo vệ pháp luật trong công tác phòng chống tội phạm công nghệ cao

Hiện nay về mặt nhà nước có ba cơ quan thực hiện chức năng quản lý nhà nước về ATTT:

- Ban Cơ yếu Chính Phủ chịu trách nhiệm quản lý về An toàn mật mã
- Bộ Công An quản lý về đấu tranh chống tội phạm công nghệ cao
- Bộ Thông tin và Truyền thông chịu trách nhiệm quản lý thông tin truyền thông trong đó có cả lĩnh vực xác thực và chữ ký điện tử. Trung tâm ứng cứu khẩn cấp máy tính Việt nam (VNCERT) trực thuộc Bộ TT&TT là đơn vị trực tiếp tham gia công tác ATTT.

9. Chi hội ATTT phía Nam và các doanh nghiệp cung cấp giải pháp, dịch vụ ATTT

Cùng với sự bùng nổ của ngành công nghệ thông tin, vấn đề bảo mật và ATTT (ATTT) đã trở thành yếu tố hết sức quan trọng và cấp thiết. Nhận thấy thực tế đó, Hiệp hội ATTT Việt Nam (viết tắt là VNISA) đã ra đời theo Quyết định số 1078/QĐ-BNV của Bộ Nội Vụ nước CHXHCN Việt Nam ngày 14/08/2007, là tổ chức xã hội nghề nghiệp phi lợi nhuận đầu tiên hoạt động trong lĩnh vực bảo mật thông tin được nhà nước Việt Nam công nhận. VNISA tập hợp các cá nhân, tổ chức làm công tác nghiên cứu giảng dạy, ứng dụng và phát triển ATTT nhằm hướng dẫn thực hiện các chủ trương đường lối của nhà nước trong việc ứng dụng và phát triển kỹ thuật, công nghệ, ATTT, đưa ra đề xuất, khuyến nghị với cơ quan quản lý nhà nước trong việc xây dựng cơ chế chính sách phát triển ngành.

Hiệp hội ATTT Việt Nam hoạt động trong các lĩnh vực:

- Tổ chức các sự kiện, hội thảo, tọa đàm, báo cáo các chuyên đề về lĩnh vực ATTT.
- Tiến hành điều tra về ATTT trên phạm vi vùng miền và toàn quốc.
- Tổ chức tư vấn và đào tạo chuyên sâu cho các tổ chức, cá nhân về giải pháp và ứng dụng trong lĩnh vực ATTT.

- Dịch vụ tư vấn và phản biện về ATTT.
- Dịch vụ đánh giá về an ninh và bảo mật thông tin.
- Tổ chức các cuộc thi, trình diễn quốc gia về ATTT.
- Chủ trì hợp tác với các hội, các doanh nghiệp trong và ngoài nước có liên quan để trao đổi, học hỏi, chia sẻ kinh nghiệm, cùng giúp đỡ nhau không ngừng đẩy mạnh ứng dụng và phát triển lĩnh vực ATTT.

Chi hội ATTT phía Nam là cánh tay nối dài của VNISA, nơi tập hợp các hội viên đơn vị và cá nhân sinh hoạt tại khu vực phía Nam. Chi hội được chính thức thành lập từ ngày 15/09/2008, hoạt động tuân thủ theo điều lệ và chỉ đạo thống nhất của hiệp hội. Cơ cấu tổ chức của chi hội bao gồm Ban Chấp hành (BCH), Văn phòng, các ban công tác, và các ban chuyên môn.

Một trong các sự kiện có ý nghĩa lớn nhất mà VNISA tổ chức thường niên đó là Ngày ATTT Việt Nam. Ngày ATTT Việt Nam nằm trong khuôn khổ các sự kiện thường niên quy mô quốc gia của VNISA, dựa trên những tiêu chí chung của Hiệp hội và thể hiện sự gắn kết giữa Nhà nước – Xã hội – Doanh nghiệp trong lĩnh vực ATTT. Đây cũng là cơ hội tiếp cận, chia sẻ những kiến thức, công nghệ bảo mật tiên tiến nhất giữa các đơn vị tham gia.

Với tiêu chí hướng đến doanh nghiệp, hướng đến cộng đồng, ngày ATTT Việt Nam luôn vì mục tiêu nâng cao nhận thức của cộng đồng về tầm quan trọng của ATTT trong môi trường kinh doanh mới dựa trên nền tảng của các hệ thống công nghệ thông tin và truyền thông; đồng thời cũng đề cập đến những giải pháp, hạ tầng kỹ thuật cần thiết nhằm đảm bảo các yêu cầu cơ bản về ATTT đối với các tổ chức, doanh nghiệp.

Trong năm 2009, Chi hội đã thường xuyên tổ chức các buổi sinh hoạt chuyên môn theo các mảng chủ đề cụ thể định kỳ hàng tháng, là nơi để các đơn vị và cá nhân là các chuyên gia trong lĩnh vực ATTT cùng chia sẻ và trao đổi các vấn đề học thuật, cũng như triển khai và ứng dụng ATTT, nhất là ở khu vực phía Nam. Trong năm 2010, Chi hội sẽ tiếp tục các chương trình sinh hoạt định kỳ, đi kèm với việc thành lập câu lạc bộ an ninh mạng nhằm đáp ứng nhu cầu chia sẻ kiến thức ATTT trong cộng đồng chuyên gia.

Hiện nay chi hội đã nhận được sự quan tâm tham gia của nhiều hội viên, trong đó có những đơn vị đã có uy tín trong lĩnh vực ATTT, có khả năng cung cấp các dịch vụ tư vấn, đào tạo, phân phối các sản phẩm an toàn an ninh mạng, triển khai và bảo trì, hỗ trợ kỹ thuật các hệ thống ATTT.

10. Kết luận, kiến nghị

Nhằm nâng cao nhận thức và thực thi công tác đảm bảo ATTT đối với các cơ quan, doanh nghiệp và người sử dụng CNTT, chúng tôi đề xuất một số kiến nghị sau:

Đối với các cơ quan nhà nước:

1. Hoàn thiện hệ thống pháp luật.
2. Thành lập đầu mối thống nhất có thể dưới dạng một Trung tâm ứng cứu sự cố máy tính là điểm tựa cho các cơ quan, doanh nghiệp và công dân trên địa bàn Tp.HCM và khu vực liên hệ.
3. Nghiêm khắc xử lý và thi hành pháp luật đối với các tội phạm công nghệ cao nhằm răn đe và phòng ngừa tội phạm.
4. Nhà nước cần có đầu tư thích đáng cho công tác ATTT như: đầu tư cho công tác nghiên cứu về ATTT, đầu tư cho đào tạo nguồn nhân lực ATTT, đầu tư xây dựng hạ tầng đảm bảo ATTT.
5. Khuyến khích sử dụng các sản phẩm, công nghệ nội địa vì tính chất đặc thù của lĩnh vực an ninh thông tin.

Đối với doanh nghiệp:

1. Tiếp tục đẩy mạnh ứng dụng CNTT nhằm tạo sức cạnh tranh cho doanh nghiệp, đồng thời nâng cao nhận thức ATTT là tài sản của doanh nghiệp cho tất cả cán bộ nhân viên.
2. Phải có chiến lược đầu tư dài hạn về công nghệ, trang thiết bị và đào tạo nhân lực đảm bảo ATTT.
3. Xây dựng qui trình ATTT, áp dụng hệ thống quản lý ATTT theo tiêu chuẩn (ISO 27001, ISO 17799).
4. Có nhận định và đánh giá đúng đắn vai trò của chuyên viên đảm bảo ATTT trong doanh nghiệp.

Đối với truyền thông, báo chí:

1. Nhận thức vai trò quan trọng trong tuyên truyền phòng chống tội phạm công nghệ cao, góp phần mạnh mẽ vào công tác phòng ngừa tội phạm.

2. Tuyên truyền pháp luật về ATTT nhằm nâng cao nhận thức về ATTT đối với từng người dân.

Cuối cùng là sự cần thiết phải phối hợp chặt chẽ giữa các cơ quan quản lý Nhà nước, các doanh nghiệp cung cấp giải pháp, dịch vụ ATTT, các cơ quan doanh nghiệp ứng dụng CNTT và Hiệp hội ATTT VNISA cũng như các hội ngành nghề khác trong lĩnh vực CNTT nhằm chia sẻ và sẵn sàng hỗ trợ khi cần thiết để thực thi công tác ATTT

Chi hội ATTT phía Nam mong muốn được đóng góp một phần công sức vào sự nghiệp chung nhằm nâng cao nhận thức về ATTT và đảm bảo ATTT cho các cơ quan, doanh nghiệp và các cá nhân vì sự bình an của xã hội và vì sự phát triển an toàn bền vững của các cơ quan doanh nghiệp.

CÔNG TÁC ĐẢM BẢO AN TOÀN AN NINH THÔNG TIN CHO CÁC CƠ QUAN NHÀ NƯỚC TRÊN ĐỊA BÀN THÀNH PHỐ

(Ông Nguyễn Anh Tuấn, Phó Giám Đốc Sở TT-TT TP.HCM)



I. HIỆN TRẠNG CÔNG TÁC TRIỂN KHAI AN TOÀN BẢO MẬT

1. Kết quả xây dựng hệ thống thông tin tác nghiệp của thành phố

Tính đến tháng 11/2009, thành phố đã đạt nhiều kết quả to lớn trong việc xây dựng hệ thống thông tin tác nghiệp phục vụ chính phủ điện tử:

a. Hệ thống hạ tầng công nghệ thông tin

Hiện tại đã có 34 sở ngành và 22 quận huyện được đầu tư xây dựng hạ tầng CNTT đảm bảo vận hành hệ thống đang triển khai tại các đơn vị, bao gồm máy trạm 5.200 bộ; máy chủ 280 bộ, Switch các loại 380 bộ, Máy in: 1.922 bộ, Kiosk tra cứu thông tin 12 bộ và hệ thống mã vạch 19 bộ;

Hệ thống Mạng MetroNet tốc độ cao kết nối toàn bộ 90 Sở/Ngành, Quận/Huyện và hơn 100 Phường/Xã, đồng thời đưa vào vận hành hệ thống điều khiển mạng MetroNet (NOC) và hệ thống giám sát đặt tại Sở Thông tin và Truyền thông (TT - TT).

b. Các hệ thống dùng chung của thành phố:

Trong năm 2009, nhiều hệ thống dùng chung của thành phố đã đi vào hoạt động, cung cấp nhiều tiện ích phục vụ công tác của cán bộ công chức thành phố:

Hệ thống thư điện tử của thành phố: chính thức vận hành từ tháng 1/2009, với năng lực cung cấp lên đến 10.000 hộp thư, phục vụ nhu cầu trao đổi thông tin giữa khối Đảng và khối chính quyền các cấp của thành phố với hơn 9000 người dùng.

Cổng thông tin thành phố - HCM CityWeb (<http://www.hochiminhcity.gov.vn>): Là cổng thông tin chính thức của chính quyền và nhân dân thành phố. Hệ thống có 77 trang Web thành viên thuộc các Sở/Ngành, Quận/Huyện của thành phố với rất nhiều thông tin phong phú: Tình hình kinh tế - xã hội, văn hóa trên địa bàn thành phố, Quy trình quản lý Nhà nước: đóng thuế, hoàn thuế, đăng ký thành lập doanh nghiệp, xin cấp phép xây dựng... Từ ngày 20/5/2009, Giám đốc Sở TT - TT được Ủy ban nhân dân thành phố giao trực tiếp quản lý, điều hành toàn bộ hoạt động hệ thống.

c. Phần mềm tác nghiệp:

Đã triển khai hệ thống các phần mềm tác nghiệp phục vụ hầu hết các lĩnh vực quản lý:

Tại các quận - huyện:

Phần mềm xây dựng môi trường làm việc điện tử (G2E): 4 phần mềm;

Phần mềm dịch vụ công (G2C và G2B): 5 phần mềm;

Phần mềm về quản lý đất đai - xây dựng (ứng dụng GIS): 8 phần mềm;

Phần mềm quản lý hộ tịch đã triển khai đến cấp phường xã.

Tại các sở - ngành:

Hiện có 5 đơn vị, gồm Sở Kế hoạch và Đầu tư, Sở Thương mại, Sở Văn hóa Thông tin, Sở Tư Pháp, Sở Khoa học và Công nghệ đã triển khai 23 phần mềm quản lý và 10 dịch vụ công phục vụ cho công tác quản lý chuyên môn. Hiện thành phố cũng đang nghiên cứu 17 phần mềm ứng dụng mã nguồn mở và đã sử dụng 6 phần mềm phục vụ cho công tác quản lý hành chính và tích hợp thông tin.

d. Cơ sở dữ liệu: đã xây dựng được cơ sở dữ liệu về: dân cư, kinh tế, văn hóa, lao động, đất đai, xây dựng... và sẽ triển khai, vận hành các phần mềm tại các Quận/Huyện, Sở/Ngành.

2. Công tác đảm bảo an toàn, an ninh thông tin cho các hệ thống thông tin tác nghiệp của thành phố:

Bên cạnh xây dựng hệ thống thông tin tác nghiệp, thành phố rất chú trọng đến công tác đảm bảo an toàn bảo mật cho các hệ thống này và đã đạt được nhiều kết quả:

a. Triển khai hệ thống bảo vệ ATTT cho các Sở/Ngành, Quận/Huyện theo mô hình chung: Nhằm thống nhất và tạo thuận tiện cho công tác đảm bảo an toàn bảo mật tại các đơn vị, ngay từ năm

2005, Sở TT - TT đã định hướng việc triển khai các hệ thống bảo vệ ATTT theo mô hình chung. Mô hình này được xây dựng qua nhiều bước, từ thí điểm, tổng kết hoàn chỉnh rồi mới nhân rộng:

Giai đoạn 1 (2005-2007): Xây dựng mô hình ở mức cơ bản, tập trung vào hệ thống chống sét, tường lửa, sao lưu dữ liệu và thí điểm triển khai chính sách ATTT. Kết quả đã triển khai cho 34 Sở/Ngành và 22 Quận/Huyện.

Giai đoạn 2 (2007-2008): Hoàn chỉnh mô hình, tập trung vào chính sách ATTT và quản lý tài nguyên hệ thống thông tin: Quản lý người dùng, Quản lý truy cập mạng, Quản lý dữ liệu...và thí điểm chính sách ATTT tại 4 đơn vị: Q.5, Q.11, Phú Nhuận và Sở TT-TT

Năm 2009: tiến hành triển khai nhân rộng trên cơ sở mô hình đã được thí điểm và hoàn chỉnh. Đến nay có 18 đơn vị được ghi vốn với tổng vốn đầu tư: 9,36 tỷ, trong đó 11 đơn vị đã được phê duyệt và triển khai dự án với tổng kinh phí phê duyệt: 4,12 tỷ.

b. Ứng dụng chữ ký số trong đảm bảo an toàn an ninh thông tin: Sở TT-TT TP.HCM là đơn vị đầu tiên trong các Sở TT-TT tiến hành xây dựng hệ thống chứng thực chuyên dùng từ năm 2006 với khả năng cấp phát 10.000 chữ ký số và bắt đầu thí điểm ứng dụng chữ ký số tại cơ quan từ 5/2006. Đến nay, đã đạt nhiều kết quả đáng khích lệ:

Gần 100 cán bộ Sở được cấp chữ ký số và trang bị mỗi cán bộ một thẻ và đầu đọc.

Tháng 10/2007, Bộ Thông tin và Truyền thông chính thức công nhận hoạt động Trung tâm chứng thực số chuyên dùng.

Chữ ký số được tích hợp vào nhiều ứng dụng thực tế như: phần mềm quản lý công văn, Tất cả văn bản của Sở TT-TT phát hành đều có chữ ký số trên file điện tử. Đặc biệt đã tích hợp chữ ký số vào kiến trúc phần mềm lõi (2008).

Năm 2009: Bắt đầu thí điểm triển khai chữ ký số tại 4 Sở/Ngành.

c. Nâng cấp hệ thống Cổng thông tin thành phố (HCM CityWeb):

Ngay sau khi được thành phố giao nhiệm vụ quản lý hệ thống HCM CityWeb, Sở TT - TT đã khẩn trương khảo sát, đánh giá tình hình hoạt động của hệ thống. Trên cơ sở đó, Sở TT - TT đã triển khai kế hoạch nâng cấp diện hệ thống nhằm đảm bảo hệ thống có thể vận hành ở mức độ cao nhất và an toàn nhất, cụ thể:

Đã xây dựng kế hoạch nâng cấp toàn diện từ hạ tầng, đường truyền, các giải pháp an toàn bảo mật đến việc nâng cấp các ứng dụng Web hiện có.

Đến nay, hệ thống hạ tầng mới cho HCM CityWeb đã được triển khai hoàn chỉnh đặt tại công ty Phát triển công viên phần mềm Quang Trung và đang khẩn trương chuyển đổi các trang Web thành viên lên hệ thống này.

Tiến hành kiểm định an toàn bảo mật các trang Web thành viên. Bước đầu đã kiểm định và khắc phục lỗ hổng bảo mật các trang Web của các đơn vị đã từng bị hacker tấn công: BQL Các Khu Chế xuất - Khu Công nghiệp (Hepza), Hội nông dân thành phố. Tiếp đến sẽ mở rộng kiểm định các trang Web của các Sở/Ngành, Quận/Huyện.

d. Công tác đào tạo về bảo mật:

Công tác đào tạo được xây dựng dựa trên nhu cầu nhân lực phục vụ triển khai các hệ thống thông tin của thành phố và Sở/Ngành, Quận/Huyện. Đến nay, đã triển khai các lớp đào tạo tập trung về an toàn bảo mật cho cán bộ quản trị các Sở/Ngành, Quận/Huyện tại thành phố và các tỉnh với kết quả đào tạo khoảng 300 cán bộ quản trị mạng (thành phố: 150, các tỉnh: 150).

3. Các tồn tại trong công tác đảm bảo an toàn, an ninh thông tin hiện nay:

Bên cạnh các kết quả đạt được, hiện nay công tác đảm bảo an toàn an ninh thông tin của thành phố còn nhiều tồn tại như:

a. Kỹ thuật, công nghệ lạc hậu:

Các hệ thống sau thời gian dài triển khai trở nên lạc hậu về công nghệ, kỹ thuật đồng thời xuất hiện nhiều lỗ hổng bảo mật. Đặc biệt phải kể đến Hệ thống Cổng thông tin thành phố (HCM CityWeb) xây dựng từ 2004, phần lớn các trang Web sử dụng các công nghệ cũ không đảm bảo tính bảo mật, Hệ thống máy chủ đã xuống cấp, thường gặp lỗi trong quá trình vận hành, đồng thời chưa có giải pháp toàn diện về an toàn, an ninh của hệ thống CityWeb (phần cứng, chính sách, cơ chế quản lý, ứng dụng,...) để có giải pháp xử lý triệt để.

Các đơn vị phần lớn chưa có chính sách ATTT: Mới chỉ có 4/89 đơn vị ban hành qui định ATTT hoàn chỉnh. Các đơn vị còn lại đang trong quá trình triển khai.

Không thường xuyên kiểm tra, phát hiện các lỗ hổng bảo mật, nhất là lỗ hổng bảo mật của ứng dụng. Trong phần lớn trường hợp, lỗ hổng bảo mật chỉ phát hiện sau khi đã gây ra sự cố nghiêm trọng.

Với một số lượng lớn các ứng dụng đã và đang triển khai, công tác đánh giá bảo mật và khắc phục đang đặt ra nhiệm vụ to lớn cho thành phố.

b. Nguồn nhân lực trong lĩnh vực ATTT còn hạn chế về nhiều mặt:

Lực lượng cán bộ quản trị mạng các đơn vị Sở/Ngành, Quận/Huyện: Thiếu về số lượng (Chỉ có 1, 2 người cho hệ thống mạng có đến 100 – 200 máy tính, chưa có cán bộ chuyên trách về bảo mật hệ thống) cũng như hạn chế về chuyên môn (Phần lớn cán bộ quản trị không phải chuyên ngành an toàn bảo mật).

Các công ty, doanh nghiệp chuyên ngành an toàn bảo mật: thành phố có ít nhất hơn 20 doanh nghiệp có cung cấp các dịch vụ an toàn bảo mật thông tin. Tuy nhiên chưa có đơn vị nào có đội ngũ chuyên nghiệp đủ sức đảm nhận trách nhiệm ứng cứu sự cố cho toàn bộ hệ thống chính quyền điện tử của thành phố.

c. Nhận thức về ATTT của người dùng còn thấp dẫn đến nhiều nội dung trong chính sách ATTT dù đã đơn giản hóa nhưng người dùng vẫn không thực hiện đầy đủ. Nhiều sai sót cơ bản vẫn khá phổ biến:

Không thường xuyên đổi mật khẩu máy tính cá nhân hoặc dùng mật khẩu đơn giản.

Khi kết nối các thiết bị ngoại vi (USB, SmartPhone) vào mạng máy tính không tiến hành quét virus như qui định.

Chưa lập hồ sơ đầy đủ, chi tiết về mạng máy tính hay không lưu trữ dữ liệu của cơ quan đúng nơi qui định.

d. Hệ thống bị tấn công:

Do tồn tại nhiều lỗ hổng bảo mật trong khi công tác khắc phục gặp nhiều khó khăn, đã xảy ra nhiều cuộc tấn công vào hệ thống thông tin của thành phố thời gian qua. Trong đó, nghiêm trọng nhất và ảnh hưởng sâu rộng nhất là vụ tấn công vào Hệ thống Cổng thông tin của thành phố (HCM CityWeb) bị hacker tấn công cài virus và các phần mềm gián điệp trong suốt thời gian từ 16-23/6/2009.

Hậu quả: Hàng chục dịch vụ công trực tuyến của chính quyền điện tử thành phố bị ảnh hưởng nghiêm trọng. Chỉ trong vòng 3 ngày, đã có 27/77 trang Website thành viên bị ảnh hưởng, trong đó có những trang của Sở/Ngành có nhiều dịch vụ công trực tuyến hay có số lượng truy cập lớn: Sở Kế hoạch và Đầu tư, Hải quan thành phố.. Một khối lượng lớn máy trạm của doanh nghiệp, người dân bị lây nhiễm virus khi truy cập để sử dụng dịch vụ.

Sở TT-TT đã phải huy động nhiều lực lượng của thành phố và cả nước, đến 23/6/2009 mới tạm thời khắc phục được. Tuy nhiên vẫn chưa tìm ra hết lỗ hổng để khắc phục triệt để. Đến nay, hacker vẫn nhiều lần tìm cách xâm nhập.

II- CÔNG VIỆC SẮP TỚI

1. Trọng tâm công việc:

Trong thời gian tới, Sở Thông tin và Truyền thông tiếp tục công tác đảm bảo ATTT cho thành phố, xem đây là lĩnh vực cần ưu tiên tập trung, đặc biệt là các nội dung sau:

Các hệ thống dùng chung của thành phố: Hệ thống thư điện tử; Trung tâm dữ liệu (DataCenter); Mạng MetroNet và hệ thống điều khiển mạng MetroNet (NOC); Cổng thông tin thành phố (CityWeb);

Các ứng dụng tác nghiệp đã và đang triển khai;

Mạng máy tính tại các Quận/Huyện, Sở/Ngành;

Đào tạo chuyên sâu cán bộ quản trị về an toàn bảo mật.

2. Các giải pháp thực hiện:

Kết hợp nhiều giải pháp và nguồn lực nhằm thực hiện nhiệm vụ đảm bảo an toàn bảo mật cho thành phố

a. An ninh hạ tầng hệ thống mạng các Sở/Ngành, Quận/Huyện:

Tiếp tục nhân rộng mô hình an toàn bảo mật cho các đơn vị Sở/Ngành, Quận/Huyện. Các đơn vị sẽ triển khai hoàn chỉnh các giải pháp an toàn bảo mật về mọi mặt: Hệ thống chống sét, Hệ thống Tường lửa, IPS/IDS, Hệ thống sao lưu dữ liệu,...;

Dự kiến có 30 Sở/Ngành, Quận/Huyện được đưa vào kế hoạch triển khai dự án “Hệ thống bảo vệ ATTT” trong năm 2010.

b. An ninh ứng dụng: Tiến hành đánh giá và khắc phục lỗ hổng bảo mật hệ thống các ứng dụng đã triển khai như:

Ứng dụng Web/Portal: 77 thành viên thuộc Cổng thông tin thành phố (HCM CityWeb);

Ứng dụng tác nghiệp tại các Quận/Huyện: 26 phần mềm tác nghiệp;

Ứng dụng tác nghiệp tại các Sở/Ngành: Phần mềm lõi, phần mềm Quản lý hộ tịch, các phần mềm cấp phép,... ;

c. Xây dựng quy trình xử lý sự cố trên mạng máy tính, trong đó xác định rõ vai trò, trách nhiệm của các đơn vị liên quan như: Đơn vị chủ trì: Sở TT – TT; Các đơn vị thụ hưởng: Quận/Huyện, Sở/Ngành; Các đơn vị cung cấp dịch vụ ứng cứu: doanh nghiệp chuyên ngành an toàn bảo mật.

d. Tổ chức lực lượng ứng cứu mạng máy tính của thành phố nhằm:

Xây dựng bằng được đội ngũ và lực lượng chuyên về an toàn và an ninh thông tin tương xứng với việc ứng dụng công nghệ thông tin của thành phố.

Thường trực xử lý khi có sự cố về phần cứng, phần mềm, kết nối mạng, sự cố virus, Trojan, hacker,...

Đảm bảo ứng cứu 24/7/365.

Đảm bảo ứng cứu cho tất cả các cơ quan Sở/Ngành, Quận/Huyện trên địa bàn thành phố.

Thường xuyên kiểm tra và cảnh báo thành phố về các lỗ hổng bảo mật phát sinh trên hệ thống mạng.

Mô hình triển khai: Áp dụng nhiều hình thức nhằm huy động cao nhất lực lượng chuyên môn về an toàn bảo mật tham gia:

i) Đối với mạng máy tính các Sở/Ngành, Quận/Huyện (90 đơn vị và hàng trăm đơn vị cấp 2):

Sở TT - TT sẽ xây dựng nội dung, định mức kinh phí cho công tác duy trì, bảo dưỡng, khắc phục sự cố... về phần cứng và hạ tầng mạng và hướng dẫn các đơn vị thực hiện.

Sở TT - TT chủ trì mua và triển khai tập trung bản quyền phần mềm chống virus cho các cơ quan quản lý Nhà nước tại thành phố nhằm chọn được sản phẩm và dịch vụ xử lý sự cố lên quan đến virus, Trojan, spyware,... tốt nhất. Số lượng bản quyền dự kiến hơn 10.000.

ii) Đối với các hệ thống dùng chung của thành phố (MetroNet, HCM CityWeb, DataCenter):

Triển khai trên hệ thống hạ tầng hiện đại đặt tại Công ty phát triển công viên phần mềm Quang Trung, áp dụng nhiều công nghệ tiên tiến Cloud Computing, đường truyền MetroNet tốc độ cao, toàn bộ hệ thống hạ tầng được thiết kế có tính dự phòng cao đảm bảo vẫn hoạt động thông suốt trong trường hợp xảy ra sự cố;

Sở TT - TT sẽ tiến hành chọn lựa các đơn vị chuyên ngành an toàn bảo mật có năng lực tốt nhất thực hiện công tác ứng cứu cho các hệ thống này.

e. An ninh dữ liệu:

Bên cạnh việc trang bị các công cụ, phương tiện lưu trữ dữ liệu chuyên nghiệp tại các đơn vị Quận/Huyện, Sở/Ngành, thành phố đang triển khai xây dựng Trung tâm dữ liệu dùng chung cho toàn thành phố. Dự kiến Trung tâm dữ liệu sẽ đi vào hoạt động từ Quý II/2010. Với kiến trúc hiện đại, vận hành trên nền hệ thống mạng tốc độ cao MetroNet, đây sẽ là nơi lưu trữ dự phòng dữ liệu của các đơn vị đề phòng cho trường hợp có sự cố. Đồng thời, Trung tâm dữ liệu cũng là nơi tập hợp thông tin cho công tác khai thác (DataMining) phục vụ cho yêu cầu quản lý của thành phố sau này.

f. Đào tạo nhân lực:

Kết hợp với các Trường, Viện, các đơn vị đào tạo tổ chức các lớp đào tạo chuyên sâu về an toàn bảo mật cho cán bộ quản trị, cán bộ phụ trách ATTT tại các Sở/Ngành, Quận/Huyện, trong đó sẽ tập trung vào: Bảo mật hệ thống, bảo mật ứng dụng; Xử lý sự cố hệ thống mạng; Đánh giá bảo mật mạng; Chính sách ATTT....Dự kiến trong năm 2010 sẽ đào tạo 200 - 300 lượt cán bộ quản trị cho các đơn vị Sở/Ngành, Quận/Huyện.

BÁO CÁO CỦA ORACLE

(Ông Đỗ Thanh Bình, Technology Senior Solution Consultant, Oracle)

SECURITY INSID=OUT

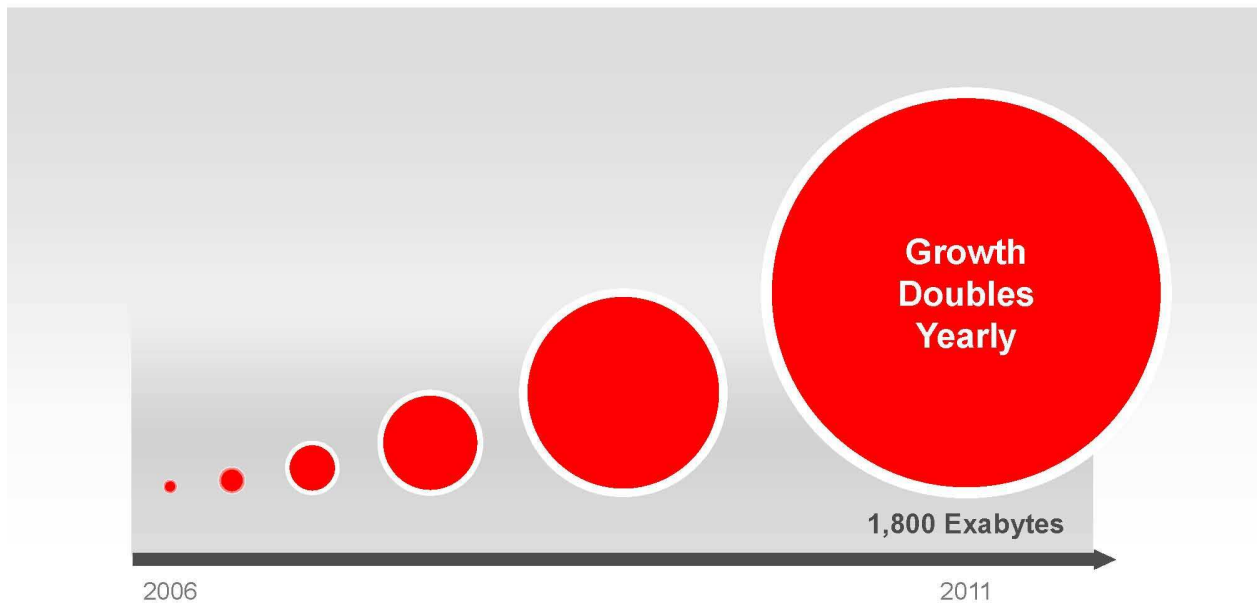
Complete Protection for Your Database,
Middleware, and Applications

ORACLE®

Database Centric Information Security

Bình Do
Technology Senior Solution Consultant

More data than ever...

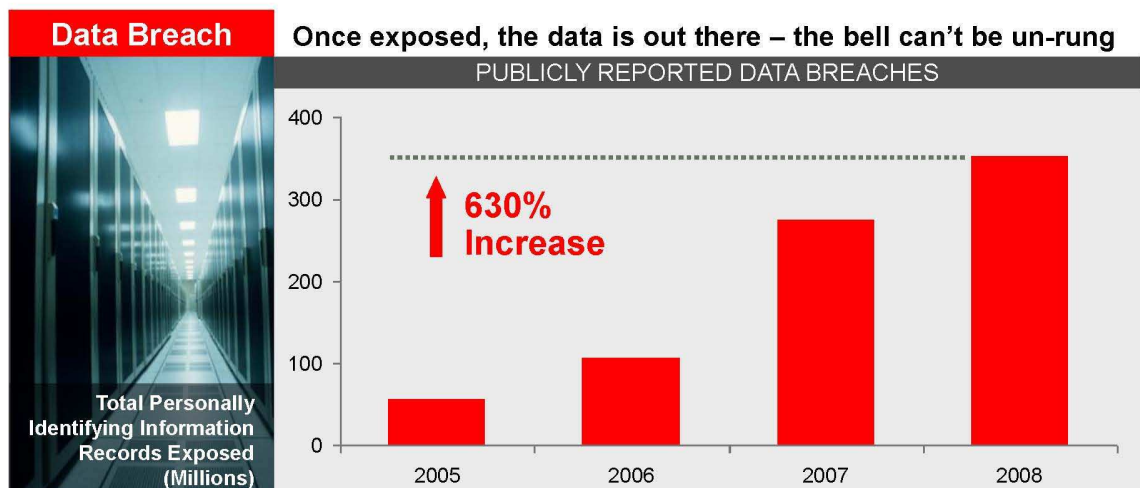


Source: IDC, 2008

ORACLE

2

More breaches then ever...

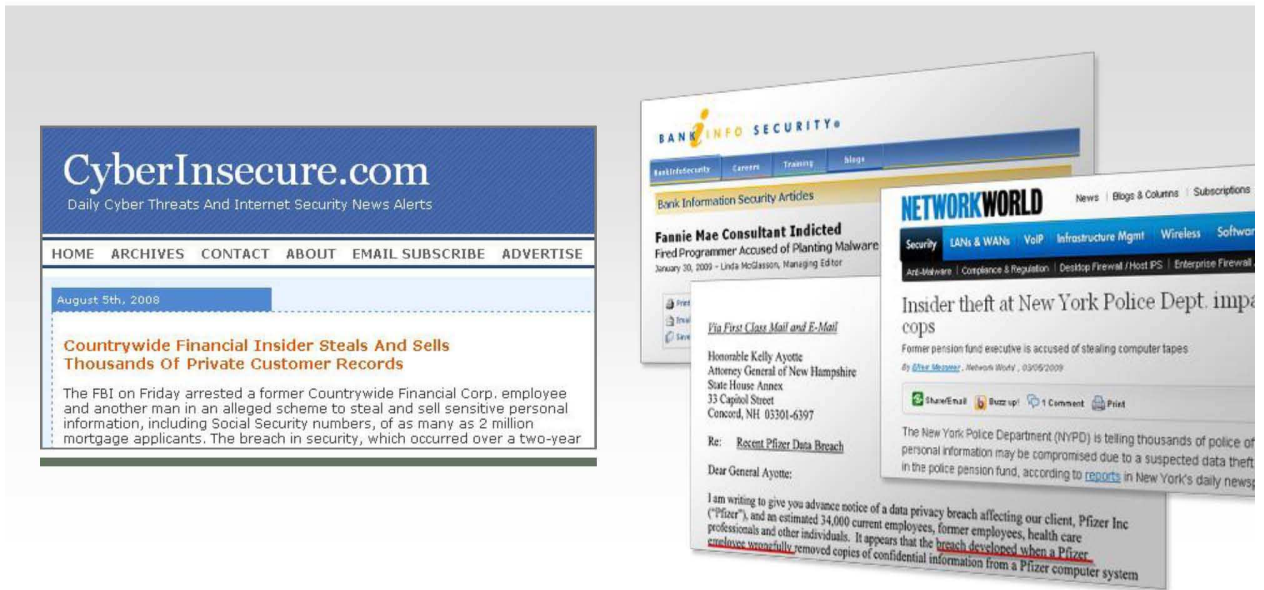


Source: DataLossDB, 2009

ORACLE

3

More threats than ever...



ORACLE

4

More Regulations Than Ever...



Source: IT Policy Compliance Group, 2007.

ORACLE

5

Market Overview: IT Security In 2009

FORRESTER®

There has been a clear and significant shift from what was the widely recognized state of security just a few years ago. **Protecting the organization's information assets is the top issue** facing security programs: **data security (90%)** is most often cited as an important or very important issue for IT security organizations, followed by **application security (86%)**.

ORACLE

6

Securing Data in Your Database

- Encryption
- Masking
- Classification
- Access Control

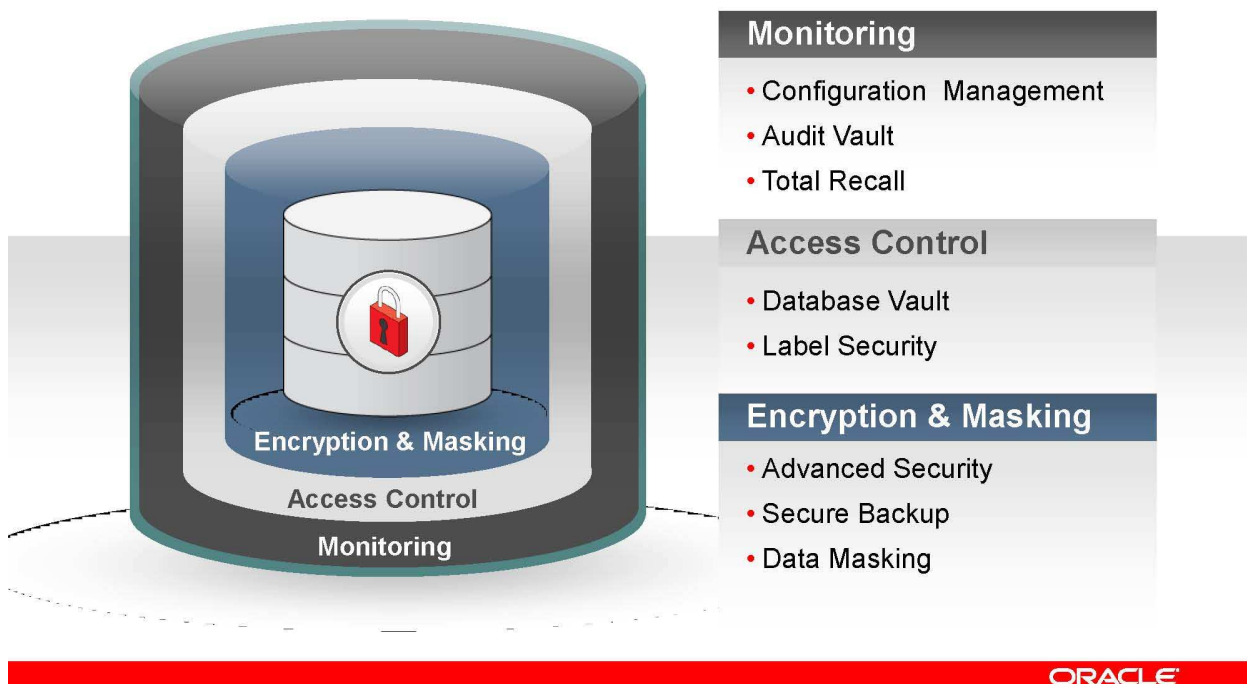


- Activity Monitoring
- Change Tracking
- Discovery and Assessment
- Secure Configuration

ORACLE

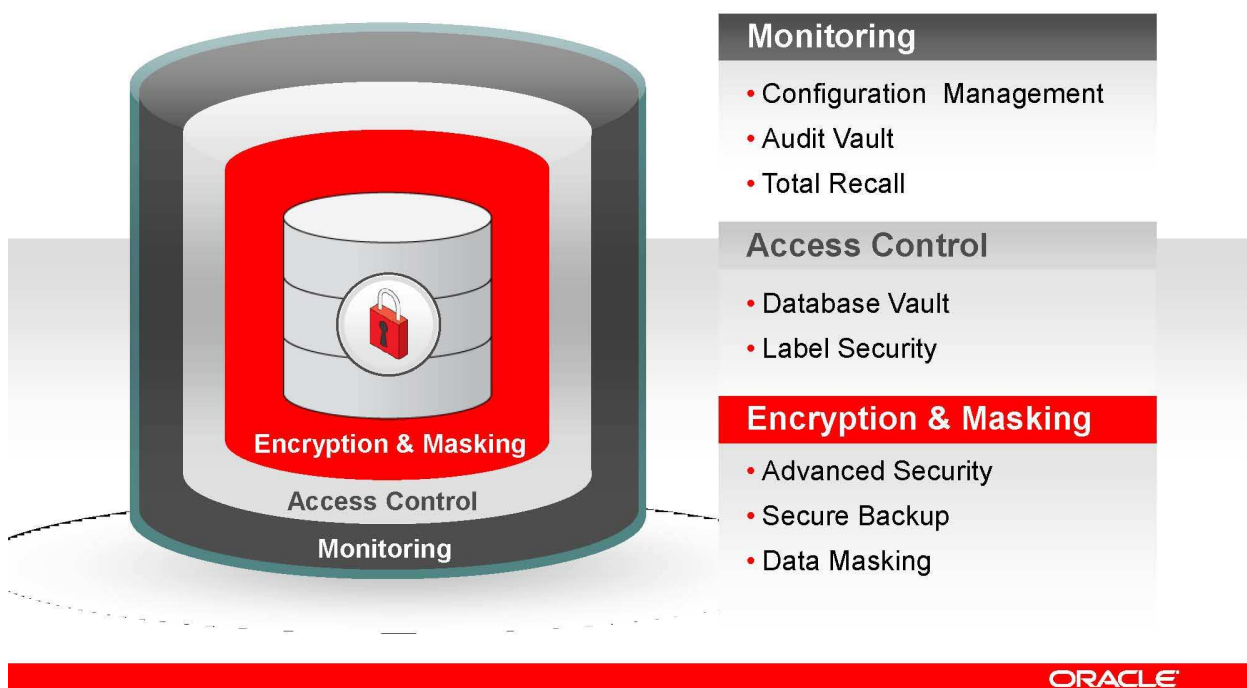
7

Database Defense-in-Depth



8

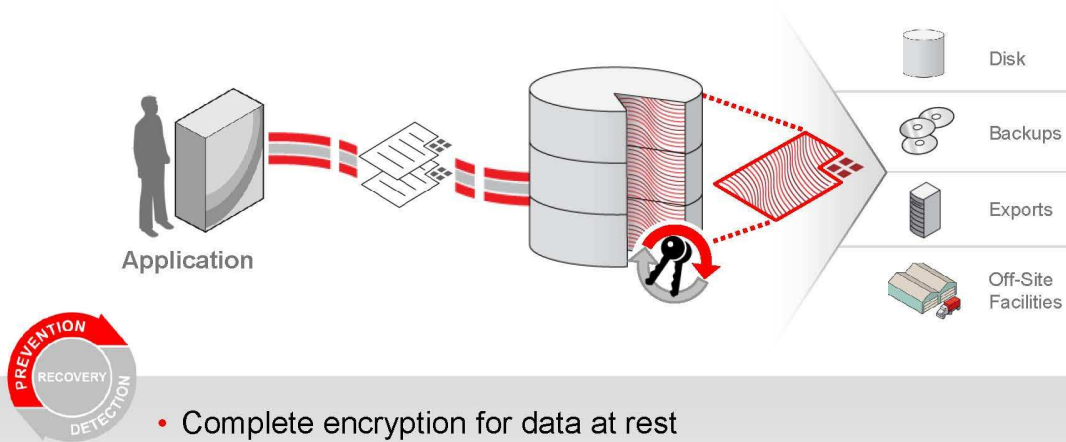
Database Defense-in-Depth



9

Oracle Advanced Security

Transparent Data Encryption



- Complete encryption for data at rest
- No application changes required
- Efficient encryption of all application data
- Built-in key lifecycle management

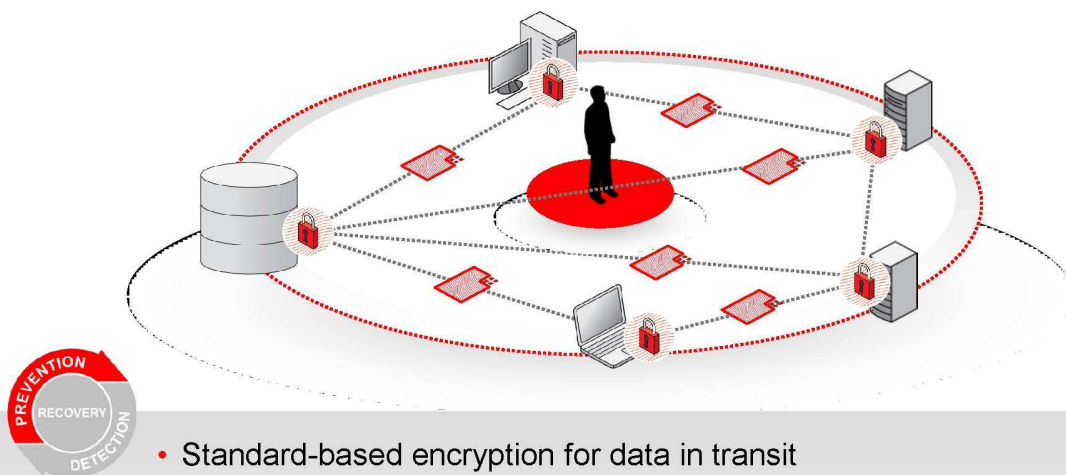


ORACLE

10

Oracle Advanced Security

Network Encryption & Strong Authentication



- Standard-based encryption for data in transit
- Strong authentication of users and servers
- No infrastructure changes required
- Easy to implement

ORACLE

11

Oracle Secure Backup

Integrated Tape or Cloud Backup Management



- Secure data archival to tape or cloud
- Easy to administer key management
- Fastest Oracle Database tape backups
- Leverage low-cost cloud storage

ORACLE

12

Oracle Data Masking

Irreversible De-Identification

Production			Non-Production		
LAST_NAME	SSN	SALARY	LAST_NAME	SSN	SALARY
AGUILAR	203-33-3234	40,000	ANSKEKSL	111-23-1111	60,000
BENSON	323-22-2943	60,000	BKJHHEIEDK	222-34-1345	40,000

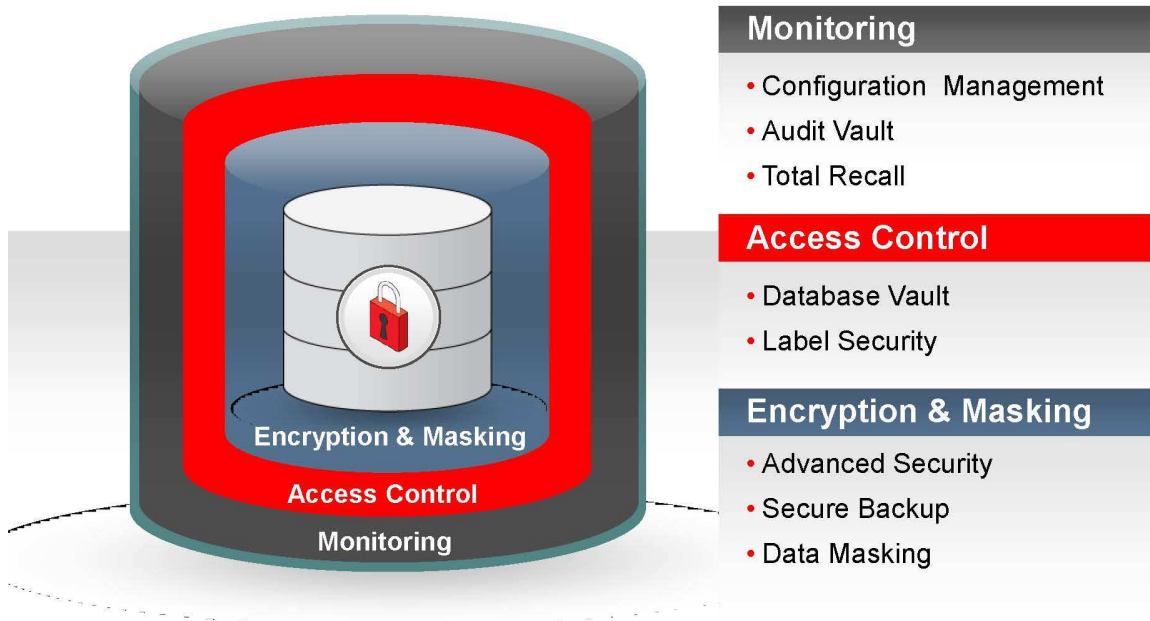


- Remove sensitive data from non-production databases
- Referential integrity preserved so applications continue to work
- Sensitive data never leaves the database
- Extensible template library and policies for automation

ORACLE

13

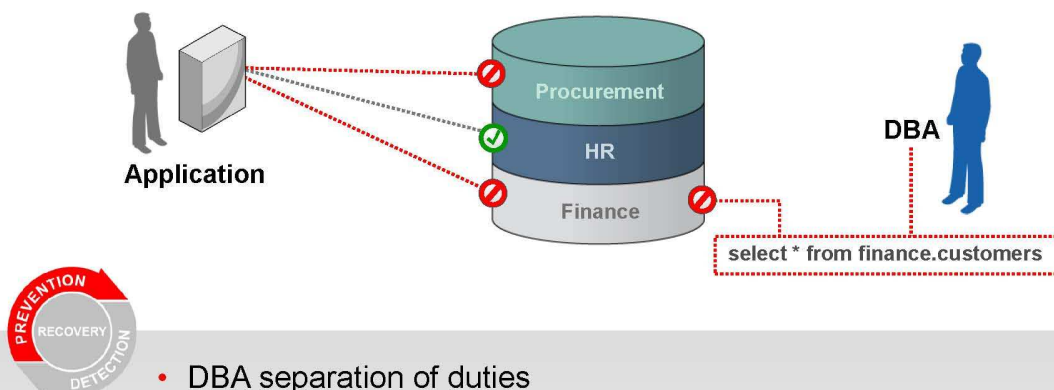
Database Defense-in-Depth



ORACLE

14

Oracle Database Vault Separation of Duties & Privileged User Controls



- DBA separation of duties
- Limit powers of privileged users
- Securely consolidate application data
- No application changes required

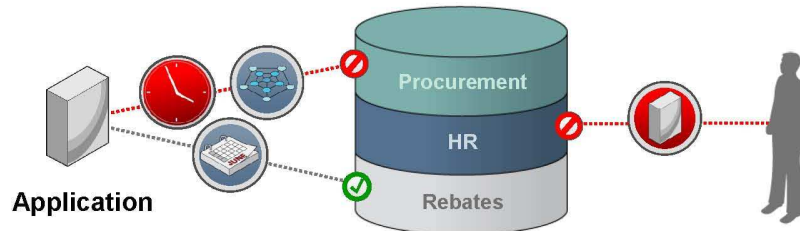


ORACLE

15

Oracle Database Vault

Multi-Factor Access Control Policy Enforcement



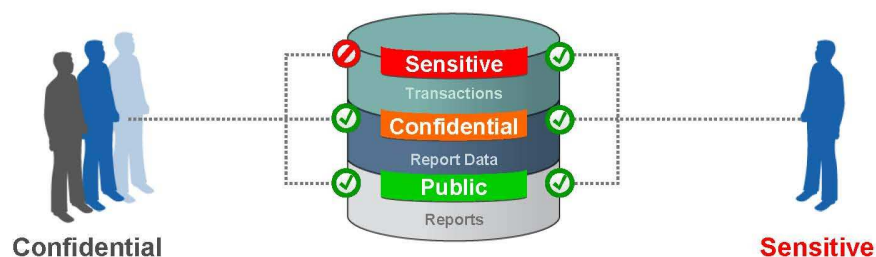
- Protect application data and prevent application by-pass
- Enforce who, where, when, and how using rules and factors
- Out-of-the box policies for Oracle applications, customizable

ORACLE

16

Oracle Label Security

Data Classification for Access Control

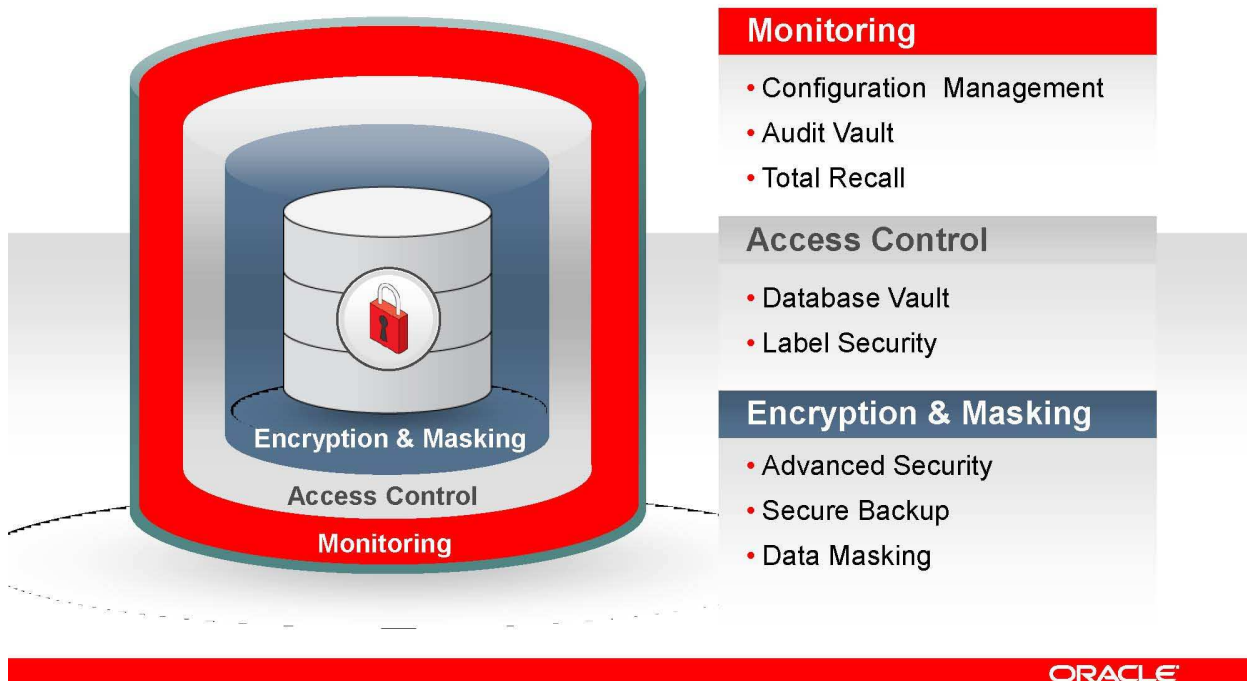


- Classify users and data based on business drivers
- Database enforced row level access control
- Users classification through Oracle Identity Management Suite
- Classification labels can be factors in other policies

ORACLE

17

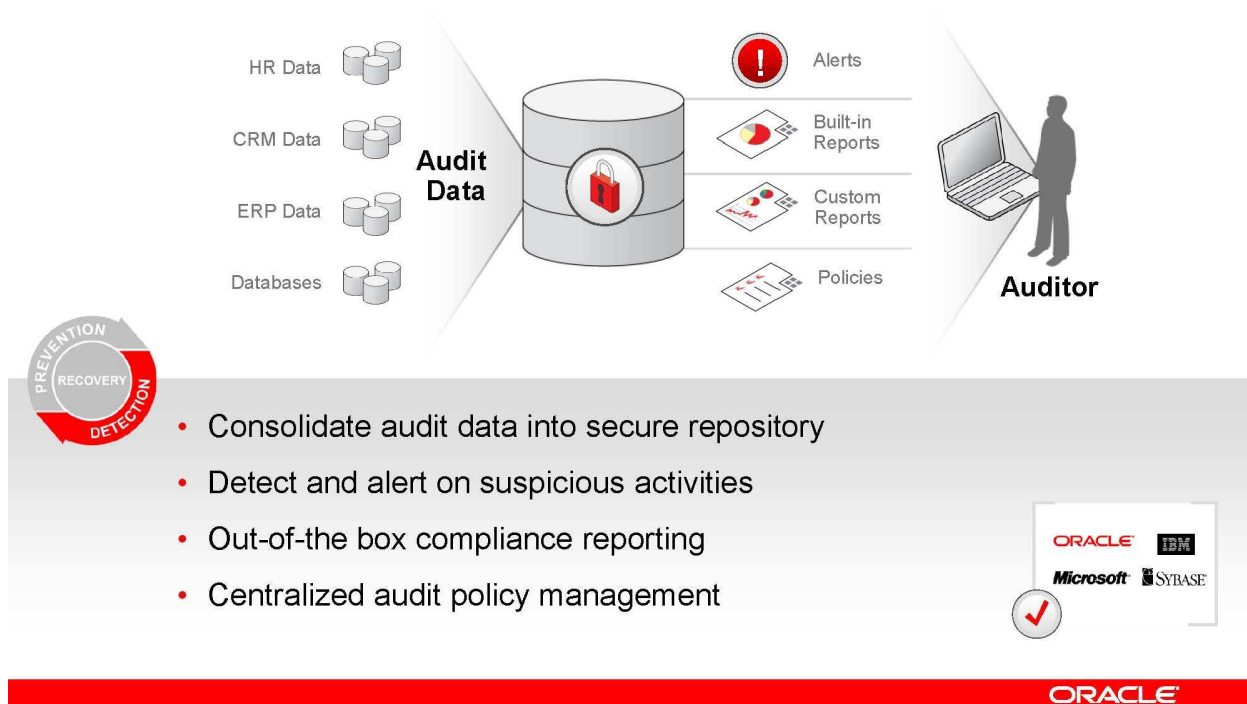
Database Defense-in-Depth



18

Oracle Audit Vault

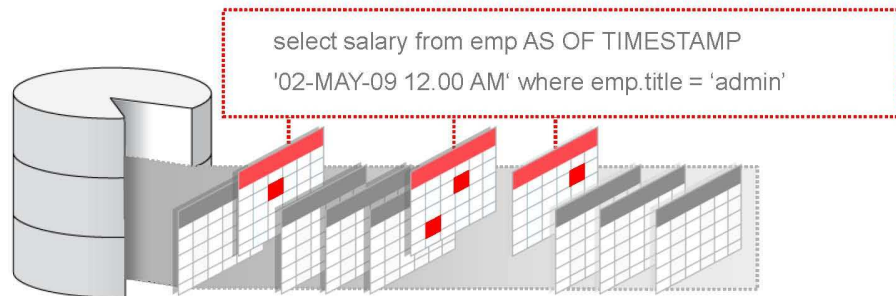
Automated Activity Monitoring & Audit Reporting





Oracle Total Recall

Secure Change Tracking



- Transparently track data changes
- Efficient, tamper-resistant storage of archives
- Real-time access to historical data
- Simplified forensics and error correction

ORACLE

20



Oracle Configuration Management

Vulnerability Assessment & Secure Configuration

Policy Group Evaluation Results

[Evaluation Results](#)
[Library](#)
[Errors](#)

This table summarizes the policy group evaluations. Click the name of the policy group for detailed information. Page Refreshed Sep 17, 2008 4:48:43

Policy Group	Version	Keywords	Average Compliance Score (%)	Targets	Type	Description
Secure Configuration for Oracle Database	1	Security	58	5	Database Instance	Ensures adherence with best-practice security configuration settings that help protect against database-related threats and attacks, providing a more secure operating environment for the Oracle database. D
Secure Configuration for Oracle Listener	1	Security	90	3	Listener	Ensures adherence with best-practice security configuration settings that help protect against database-related threats and attacks.

[Evaluation Results](#)
[Library](#)
[Errors](#)

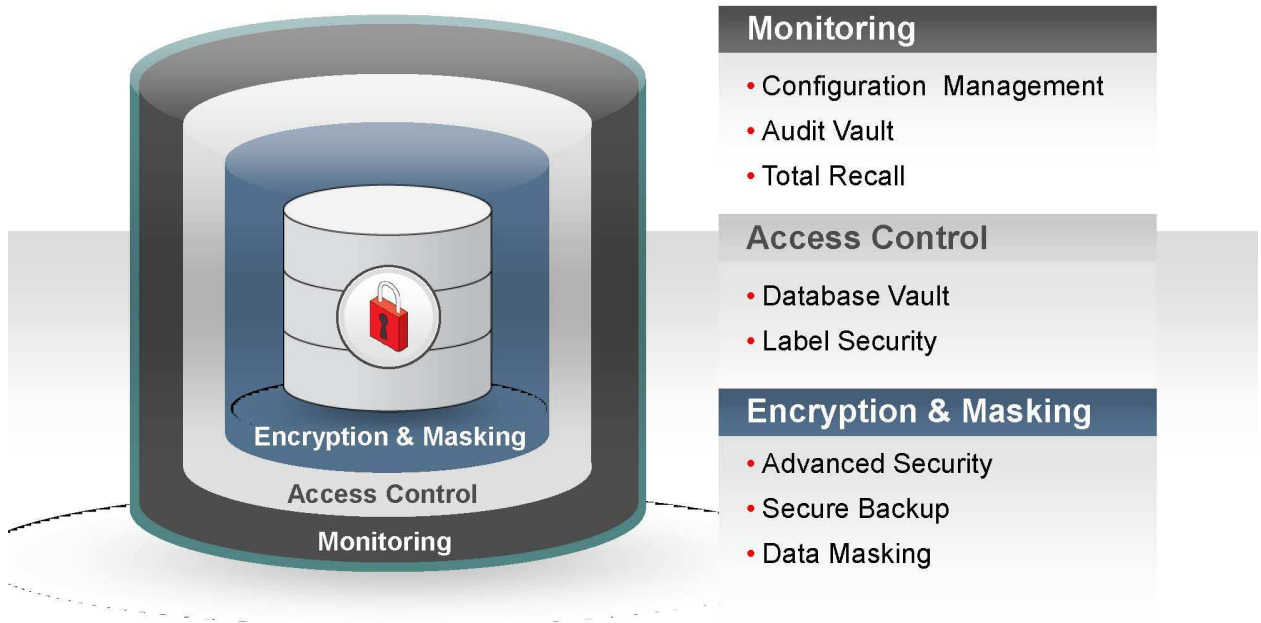


- Database discovery
- Continuous scanning against 375+ best practices and industry standards, extensible
- Detect and prevent unauthorized configuration changes
- Change management compliance reports

ORACLE

21

Database Defense-in-Depth



ORACLE

22

For More Information

search.oracle.com

Search for: In the section:

or

oracle.com/database/security

ORACLE



ORACLE

24



ORACLE IS THE **INFORMATION** COMPANY

Tóm tắt sơ lược tiểu sử Ông Đỗ Thanh Bình:



ĐỖ THANH BÌNH

Chuyên gia tư vấn cao cấp giải pháp công nghệ
Tập đoàn **Oracle**

Trình độ chuyên môn: Đại học chuyên ngành CNTT	
Kinh nghiệm công tác:	
2006 đến nay	Công tác tại tập đoàn Oracle. Phụ trách tư vấn giải pháp công nghệ về bảo mật CSDL Oracle và giải pháp điện toán lưới.
2003 – 2006	Công tác tại công ty Hyundai Information Technology với các vị trí: Quản trị hệ thống, quản trị CSDL Oracle và Quản lý dự án.
	Giảng viên giảng dạy lập trình CSDL và quản trị CSDL Oracle
	Tham gia triển khai dự án hiện đại hoá hệ thống ngân hàng
2002 – 2003	Trưởng nhóm lập trình WEB và CSDL tại công ty TECHCOM
2000 – 2002	Chuyên viên lập trình WEB và CSDL tại công ty Pháp PH-TECH

CƠ SỞ HẠ TẦNG NĂNG ĐỘNG BẢO VỆ TÀI SẢN DOANH NGHIỆP

(Đại diện công ty IBM)

Topic: A Dynamic Infrastructure that puts your business assets first

IBM introduces solutions that help enterprises to build dynamic infrastructures which then allow your business to utilize the most of the business information and assets. Doing so by not only allow:

- Easily manage to systems or applications with less resource, power consumption
- Scalability up to the business needs
- Advanced technology and features that help secure your business information and assets are well kept from threats.

Cơ sở hạ tầng năng động để bảo vệ tài nguyên kinh doanh và bảo mật thông tin

IBM giới thiệu các giải pháp kết hợp các ứng dụng công nghệ mới nhất nhằm giúp doanh nghiệp, tổ chức xây dựng một hạ tầng CNTT năng động. từ đó giúp khai thác một cách tốt nhất hiệu quả nhất các tài sản quan trọng của doanh nghiệp: thông tin và các nguồn lực kinh doanh. Các giải pháp này giúp doanh nghiệp:

- Dễ dàng hơn trong việc quản lý hệ thống và các ứng dụng với ít nguồn lực và tiết kiệm điện năng hơn.
- Có khả năng mở rộng tùy theo nhu cầu của sự phát triển
- Các cộng nghệ và chức năng tiên tiến nhất nhằm đảm bảo an toàn các thông tin và tài sản kinh doanh tránh khỏi các rủi ro, sự nhòm ngó từ bên ngoài.

TỔNG QUAN CISCO SAFE: KIẾN TRÚC AN NINH MẠNG THẾ HỆ MỚI ĐÃ ĐƯỢC KIỂM CHỨNG TRONG THỰC TẾ

(Ông Phan Thanh Sơn, Giám đốc Công nghệ Công ty Cisco Systems Việt nam)

11/12/2009




Cisco SAFE Overview:
Validated Next-Generation
Security Architecture

Phan Thanh Sơn
CTO, Cisco Vietnam

Today's Complex Security Threats Require Systemwide Collaboration

Top-Ten Cyber Security Menaces

- Sophisticated website attacks
- Increasing botnet sophistication and effectiveness
- Growing cyber espionage
- Emerging mobile phone threats
- Insider attacks
- Advanced identity theft
- Increasingly malicious spyware
- Web application security exploits
- Sophisticated social engineering
- Supply-chain attacks infecting consumer devices



Source: SANS Institute

The Greatest Security Threats

- New technologies unprotected
 - Web 2.0, virtualization, cloud computing, etc.
- Lack of consistency and collaboration across products
- Accidental architecture
 - Fear-based security decisions
 - Product- or feature-of-the-moment purchases
- Siloed products and designs
- Poor security policy, control, management, and visibility



Cisco SAFE

Security Reference Architecture
Free Technical Design and Implementation Guide

- **Security Control Framework**
 - Basis for all Security Designs
 - Focus on Visibility and Control
 - Combines Solutions and Services
- **Benefits**
 - Combines security and network
 - Fully tested and validated
 - Speeds implementation
 - Modular design



Cisco SAFE Objectives

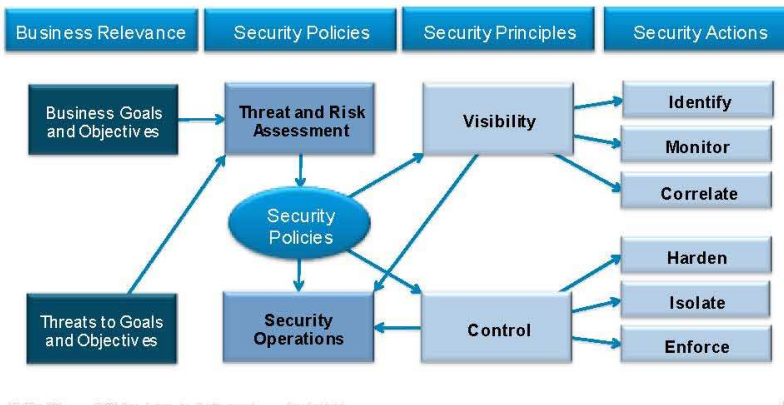
Cisco® SAFE addresses threats to critical business goals and objectives

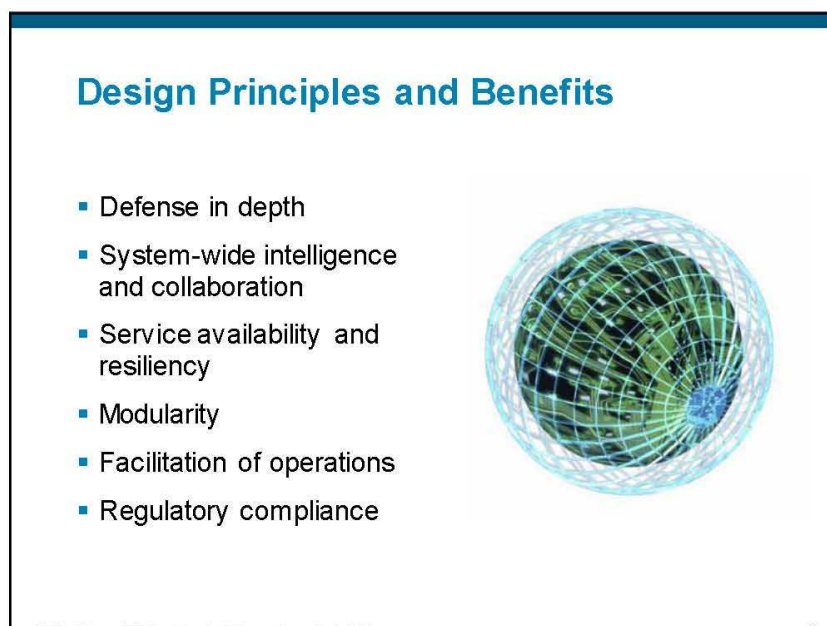
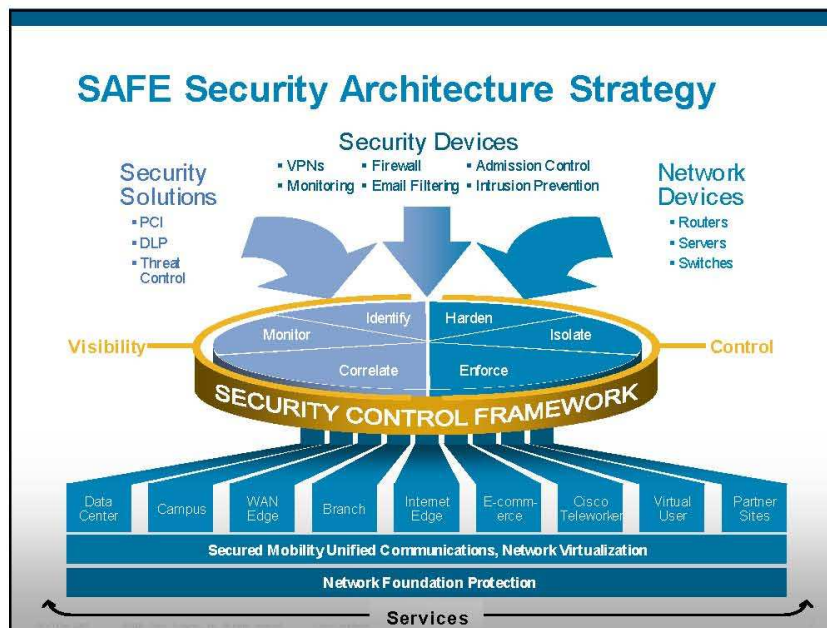
Business Goals and Objectives	Potential Threats
Protecting revenue sources	Disruption of business, resulting in loss of revenue
Meeting customer requirements	Loss of customer privacy, security, and service levels
Safeguarding corporate identity and brands	Negative effect on marketing campaigns and brand reputation
Compliance with regulations and standards	Fines, loss of business, and legal action

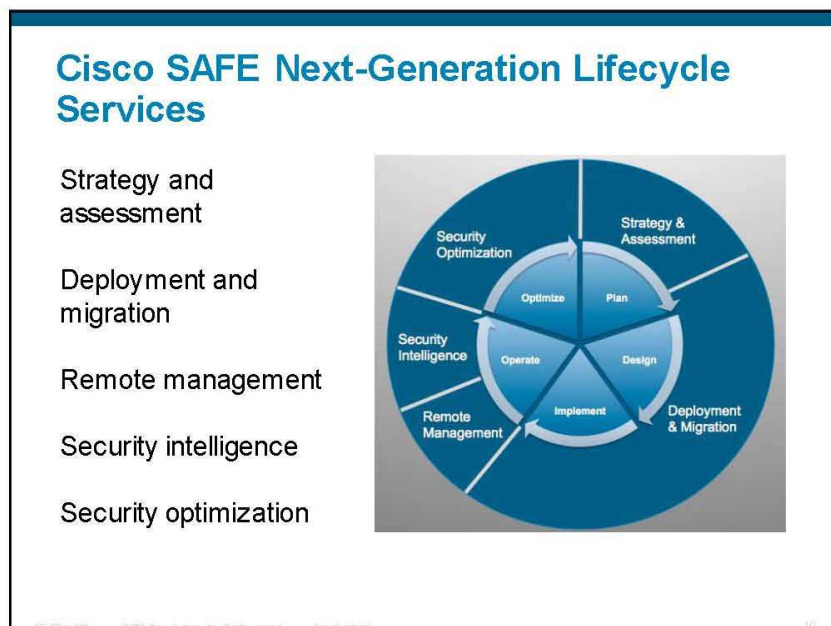
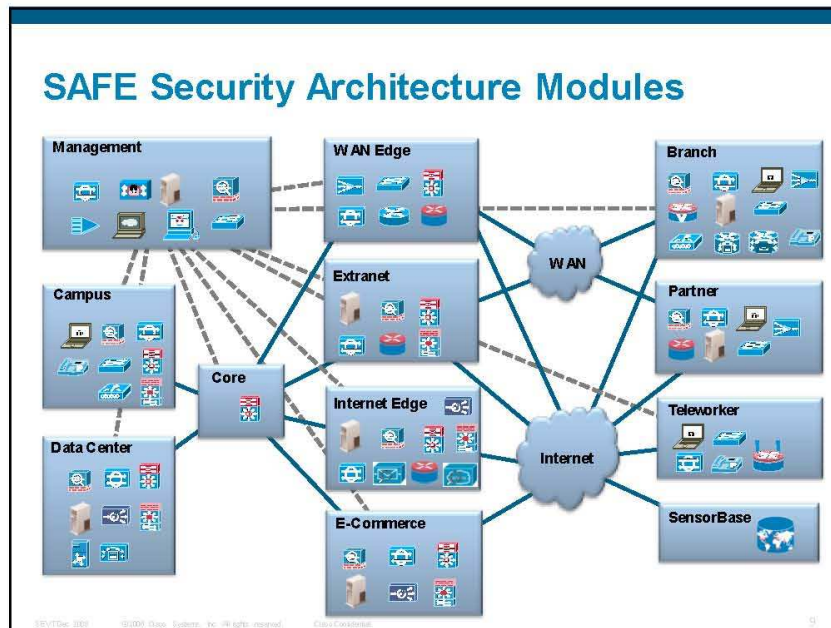
© 2009 Cisco. All rights reserved. Cisco Confidential

Cisco Security Control Framework

Cisco® SAFE designs and strategies are based on Cisco's Security Control Framework for consistent policy deployment and enforcement across the network







Cisco SAFE Benefits

- Step-by-step design and implementation guidance
- Fully tested and validated
- Solutions-based approach
- Layered security using best practices
- Threat visibility and coordinated response
- Assurance of business-critical service availability
- Modularity to support strategic improvement
- Compliance with regulatory requirements



© 2009 Cisco. All rights reserved. Cisco Confidential

10

SAFE Resources

- Cisco SAFE:
<http://www.cisco.com/go/safe>
- Cisco Design Zone:
<http://www.cisco.com/go/cvd>
- Cisco Security Lifecycle Services:
<http://www.cisco.com/go/services/security>
- Cisco's Security Products:
<http://www.cisco.com/go/security>

© 2009 Cisco. All rights reserved. Cisco Confidential

11

Cisco SAFE: A Security Reference Architecture

The Changing Network and Security Landscape

The past several years have seen tremendous changes in the network, both in the kinds of devices being deployed and in the network services that are available. Innovations such as virtualization, cloud computing, and web-based access for employees, partners, and customers are bringing about a dramatic evolution in nearly every organization's infrastructure. Many organizations are also transitioning from physical-based collaboration processes to collaborating across geographies by building distributed networks to gain a time-to-market advantage.

The technology supporting these advances also continues to evolve. Bandwidth is ubiquitous. Workers are becoming more and more mobile because they have the devices and networks to do so. Web 2.0 technologies and service-oriented architectures (SOAs) are creating new ways to work and collaborate, and to reach out to customers and partners.

From a security standpoint, these changes have brought with them several new and complex challenges. Traditional point security tools are limited in their ability to support and secure this business transformation, either leaving critical new resources unprotected or preventing the deployment of new services because they do not secure new processes and protocols. At the same time, organizations are facing a host of new threats that target many of these new services and impact network and service availability; these include the theft of identity, data, and reputation, and the abuse of application and network resources.

Today's new threats share several characteristics. They are complex, targeted at specific networks, and increasingly focused on exploiting new applications and services. They include:

- Increasing botnet sophistication and effectiveness
- Emerging mobile phone threats
- Advanced identity theft
- Increasingly malicious spyware
- Web application security exploits
- Supply chain attacks infecting consumer devices

The increase in rigid security regulations further complicates securing the network, and has left many organizations wondering how to balance increased compliance requirements with expanding critical business services. A partial list of regulations includes Sarbanes-Oxley (SOX), Payment Card Industry Data Security Standard (PCI DSS), Graham-Leach-Bliley Act (GLBA), Health Insurance Portability and Accountability Act (HIPAA), Federal Information Security Management Act (FISMA), U.S. PATRIOT Act, Personal Information Protection and Electronic Document Act (PIPEDA), Japan Personal Information Protection Act (PIP), Australia Federal Privacy Act, Basel II, and EU Data Protection Directive (EU DPD).

Common Security Mistakes

Failure to address security in terms of securing and enabling specific business processes can leave organizations with serious security vulnerabilities. Some of the largest, yet most overlooked threats to organizations lie within their own networks. Here is a brief overview of some of the most common security mistakes organizations make:

Siloed Products and Design

This happens when an organization's security infrastructure is comprised of a host of legacy security products purchased over a period of time and loosely coupled together. The problems caused by this type of security architecture include:

- No central command and control
- Poor visibility into the network's health
- Inability to collect and share critical security event information
- Little to no collaboration between elements to address threats
- No real integration between security and network components
- High IT overhead for managing and maintaining siloed security elements

Fear-Based Security Decisions

Often, organizations fall into the trap of focusing on unlikely, high-profile threats rather than more common threats. While these organizations may be quite adept at thwarting a new Internet worm, for example, they often overlook more mundane security issues, such as turning off unused ports, preventing insider abuse and misuse, or detecting rogue wireless access points. Of course, addressing high-profile security events is important, but true risk management must be part of a comprehensive security strategy that sees the network, network services, and security elements as part of a greater whole.

Products vs. Risk Management

Another oversight many organizations make is selecting security products based solely on feature-to-feature comparisons. The reality is that all products are in a constant state of development, and any one product may have, at any moment in time, a particular feature that another product doesn't. In another six months, this sort of comparison is likely to yield completely different results. Instead, security products should all be evaluated on the criteria of risk management to ensure that the security element you acquire meets, as much as possible, the business risks and requirements of your unique environment, now and into the near future.

Inadequate Security Policy

The most essential foundation for any security strategy is an intelligent security policy. Unfortunately, for many organizations, a security policy either doesn't exist, or was an exercise completed some time ago that has been largely unused and perhaps ignored since its creation. Another common security policy error is that it is often focused on the placement of products in the network, paying little attention to supporting and securing the organization's network and business strategy. The result is a document that is not focused on the dual goals of business enablement and continuity, and maximum risk reduction, and that fails to provide guidelines for maintaining management, control, and visibility.

Risk Management

Risk management includes the assessment, mitigation, and monitoring of threats to keep risk at an acceptable level. Any risk management strategy needs to consider the following security priorities:

- **Protection of revenue sources:** Business disruptions caused by network outages and attacks may result in loss of revenue, both in terms of direct business conducted over the network and in the loss of consumer confidence due to publicized security breaches.
- **Addressing customer requirements:** Customers are increasingly concerned about the protection of their private and personal information. Threats to customer privacy, a loss of a sense of security or confidence, and reduced service levels can all adversely affect the corporate bottom line.
- **Safeguarding corporate identity and brands:** Security breaches and attacks, especially high-profile attacks, can have a significant impact on marketing campaigns, brand reputation, and confidence in the organization.
- **Compliance with regulations and standards:** Failure to comply with increasingly stringent legal and corporate regulations and standards can lead to stiff fines and penalties, loss of business, and legal action.

To address these issues, it is essential to make sure that current and future business processes are understood so that security implementations can be designed to support and defend them. Before evaluating any security product or creating or amending any security policy, a few simple questions need to be asked:

- Are business processes well-understood? Are there sufficient safeguards in place to protect data at rest, in transit, and in use?
- What business applications, services, and infrastructure changes are being deployed or may be deployed in the next several years?
- What are the risks associated with implementing those solutions?
- How do we reduce those specific risks as much as possible?
- What regulatory compliance mandates are required for the organization, and what is the plan for meeting them?

In answering these questions, organizations have traditionally been left on their own, largely because traditional security vendors only provide a narrow, "siloeed" product to address a broad and integrated problem. Clearly, what is needed is specific guidance, based on best practices and validated designs, on how to discuss, design, and implement a coherent and consistent security solution.

Cisco SAFE Architecture

Cisco has updated its security reference architecture, called Cisco® SAFE, to provide detailed design and implementation guidelines for building secure and reliable network infrastructures and the policies that support them. These guides are based on security best practices combined with thousands of hours of design, testing, and documentation.

A network isn't a single entity, but rather a collection of network elements, such as the data center, campus, or branch—each with specific functions and security requirements. The Cisco SAFE architecture takes a modular approach in order to best address the unique needs of different places in the network, as well as the critical interoperations between them. This modularity also extends

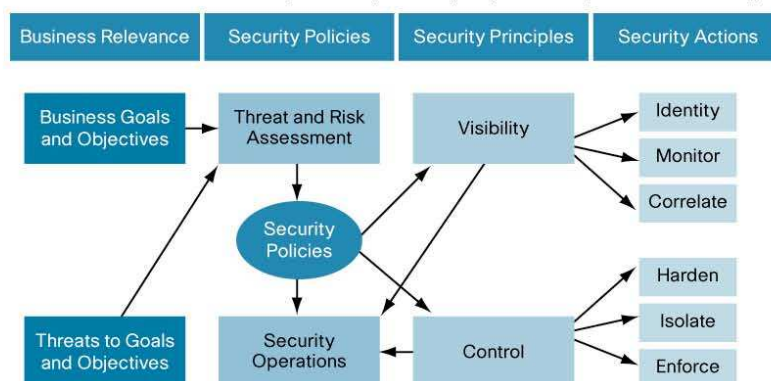
the useful life of existing equipment, protecting previous capital investments. The designs also incorporate a set of tools to facilitate day-to-day operations, thereby reducing overall operational expenditures.

In today's threat environment, everything is a target. Because of this, Cisco SAFE takes a defense-in-depth approach to security. SAFE's systemwide intelligence approach addresses the security of the infrastructure; endpoints; network devices; applications and application servers; databases; web, email, and other servers; communications devices; and storage systems. It does this by emphasizing the integration of security into each of these components, so rather than being targets, each component contributes to the health of the network, the strategic placement of purpose-built security products, and the collaboration between these elements to create systemwide intelligence and improve visibility and control. Finally, SAFE's secure management and reporting design provides a unified strategy for enforcing policy and for monitoring, analyzing, and responding to threats.

Cisco SAFE design principles not only focus on providing deeper security within specific places in the network, but also between and among functional network zones, as data and transactions traverse the entire infrastructure. Event and posture information is shared among devices and across safeguards for greater visibility, with response actions coordinated under a common control strategy.

The Security Control Framework

SAFE's underlying strategy is the Security Control Framework, a standardized approach to security policy development and deployment. Security Control Framework principles and actions are used to identify the most appropriate technologies and best common practices to secure the unique environment of each place in a network. The result is that multiple security technologies and capabilities are used together throughout the network to gain visibility into network activity, enforce network policy, and address anomalous traffic. In addition, network infrastructure elements such as routers and switches are used as pervasive, proactive policy monitoring and enforcement agents.



Two fundamental principles of the Security Control Framework are maximizing visibility into the devices and events on the network, and control of the users, devices, and traffic moving across the network. Under the categories of visibility and control, the Security Control Framework defines six security actions to enforce security policies.

Visibility

1. Identify and classify users, services, traffic, and endpoints.
2. Monitor performance, behaviors, usage patterns, events, and policy compliance.
3. Collect, analyze, and correlate systemwide events.

Control

4. Harden endpoints, services, servers, applications, and infrastructure.
5. Isolate users, systems, and services when containment is needed.
6. Enforce access controls and security policies, and mitigate security events.

Planning, Review, and Improvement

Because business and security needs are always evolving, another key principle of the Security Control Framework is the ongoing review and adjustment of any security implementation to continually meet changing security and business requirements. There are five key steps in the Security Control Framework development and review process:

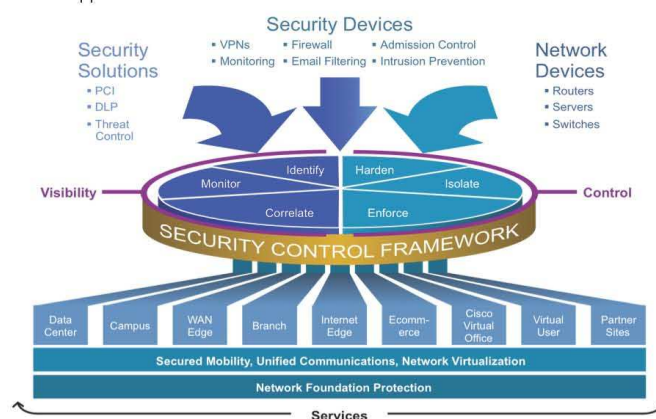
1. Plan. The planning stage must include a threat and risk assessment aimed at identifying assets and the current security posture. Planning should also include a gap analysis to unveil the strengths and weaknesses of the current architecture.
2. Design. Next is the creation of a detailed design that includes the selection of the platforms, capabilities, and best practices needed to close the gaps identified in the planning assessment, and to satisfy future business and technical requirements.
3. Implement. This includes the deployment and provisioning of platforms and capabilities, as well as hardening the underlying network infrastructure. Deployment is typically executed in separate phases, which requires plan sequencing.
4. Operate. Maintenance of the new security implementation includes the management and monitoring of the infrastructure, as well as gathering, reviewing, and responding to security intelligence for consistent and timely threat mitigation.
5. Maintain. Regular plan reviews need to be conducted to identify and address gaps resulting from changes or additions to the network environment. The information obtained from day-to-day operations and from ad-hoc assessments can be used for these purposes. A risk and threat reassessment needs to be periodically conducted. Results from this reassessment lead to restarting the solution cycle, to constantly improve the security architecture and better meet evolving business and security policy needs.

For many organizations, this process can be a daunting task, both in terms of the expertise required and the commitment of IT resources. To that end, Cisco Services has created a complementary suite of services designed to assist in each of the five steps recommended by the Security Control Framework, as well as in the ongoing lifecycle management of any SAFE deployment.

The SAFE Security Architecture

Cisco SAFE comprises a series of validated, end-to-end security design and technical implementation guides that are made available, free of charge, to any organization looking for guidance on developing or improving the security of their networked environment. Some of the key benefits of the Cisco SAFE design and implementation guides include:

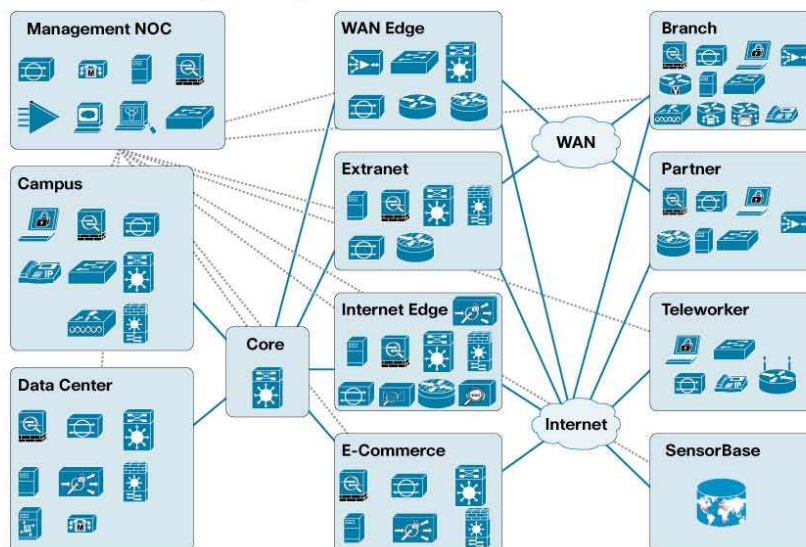
- Detailed designs, based on best practices and real-world testing and validation, help organizations move more quickly from concept to implementation. They also help frame discussions about how to create and improve security policy. By removing much of the guesswork that has traditionally gone into securing a network infrastructure, organizations can realize significant savings from the costs that can result from trial-and-error attempts to create a secure environment.
- Modular designs, based on securing the unique needs of specific places in the network, support incremental improvement over time. Most organizations are not in a position to overhaul their entire security infrastructure. Because of SAFE's modular approach, however, organizations can begin to improve their security profile by updating only that portion of the network most in need of improvement. And because the various components of SAFE are part of an integrated strategy, as each place in the network is improved, the overall visibility, control, and health of the network also improve incrementally and holistically.
- Defense-in-depth secures against more complex threats. With multiple vector attacks, many of the individual attacks either slip past security gaps or are identified as low-level concerns and ignored. Cisco's collaborative security design allows different devices to not only share threat information, but also to aggregate information to detect, report on, and thwart these more complex threats.
- Detailed, step-by-step architectural and platform-specific guidance reduces the IT costs associated with design, deployment, and implementation.
- Collaboration between security elements and the network infrastructure not only creates strong security, but also helps ensure network availability and support for key business applications and network services.



SAFE Network and Solution Modules

The SAFE architecture delivers defense-in-depth by strategically deploying Cisco products and capabilities across the network and by taking advantage of the collaborative nature between platforms. Multiple layers of security technologies are deployed under a common strategy and administration. Products and capabilities are positioned where they deliver most value and to best facilitate collaboration and operations.

Here is an overview diagram of the places in the network included in the Cisco SAFE architecture:



Design guidance is also provided for technologies or elements present across multiple places in the network, such as unified communications, network virtualization, mobility solutions, data loss prevention, identity management services, and network foundation protection.

Cisco Lifecycle Security Services for SAFE

Cisco offers services for the SAFE architecture that are based on an approach that considers the entire lifecycle of a SAFE security deployment, from initial assessment to deployment to operations and optimization. These lifecycle support services address the following phases of a SAFE deployment:

- **Strategy and assessment:** Cisco offers a comprehensive set of assessment services based on a structured IT governance, risk management, and compliance approach to information security. These services help companies understand the needs of and gaps in their network security architecture. Recommendations are based on industry and international best practices. These services help companies to strategically plan the evolution of an information security program, including updates to security policy, processes, and technology.
- **Deployment and migration:** Cisco offers deployment services to support companies in planning, designing, and implementing Cisco security solutions. In addition, these services can help companies in evolving their security policy and process-based controls to make the security architecture more effective while supporting efforts to increase productivity and collaboration among network users.
- **Remote management:** Cisco Remote Management Services engineers become an extension of a company's IT staff, proactively monitoring the security technology infrastructure and providing incident, problem, change, configuration, and release management, as well as management reporting 24 hours a day, 365 days a year.

- **Security intelligence:** Cisco Security Intelligence Operations services provide early warning intelligence, analysis, and proven mitigation techniques to help security professionals respond to the latest threats. Cisco experts use in-depth knowledge and sophisticated tools to verify anomalies and develop techniques that help ensure timely, accurate, and quick resolution to potential vulnerabilities and attacks.
- **Security optimization:** The Cisco Security Optimization Service is an integrated service offering designed to assess, develop, and optimize a company's security infrastructure on an ongoing basis. Through quarterly site visits and continual analysis and tuning, the Cisco security team becomes an extension of the company's security staff, supporting them in long-term business security and risk management, as well as near-term tactical solutions to evolving security threats.

Conclusion

Cisco SAFE provides a much-needed holistic approach to securing the entire network environment. Its comprehensive security strategy improves an organization's ability to identify, prevent, and respond to threats. But just as important, SAFE enhances an organization's ability to securely deploy critical business applications and services that enable collaboration, increase productivity, and better address the increasing demands of customers, competitors, partners, and employees.

Cisco SAFE Resources

- Cisco SAFE: <http://www.cisco.com/go/safe>
- Cisco Validated Design Program: <http://www.cisco.com/go/cvd>
- Cisco Security Lifecycle Services for SAFE: <http://www.cisco.com/go/services/security>
- Cisco security products: <http://www.cisco.com/go/security>



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

CCDE, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CQVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0812F)

Printed in USA

C11-527476-00 04/09



Cisco SAFE Reference Guide

Cisco Validated Design

Revised: August 20, 2009, OL-19523-01

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-19523-01

Tóm tắt sơ lược tiểu sử Ông Phan Thanh Sơn:

Ông Phan Thanh Sơn là Giám đốc Công nghệ (CTO) của Công ty Cisco Systems Việt nam. Sơn đã có 17 năm kinh nghiệm làm việc trong ngành Công nghệ thông tin – Truyền thông (ICT). Ông đã tham gia tư vấn và thiết kế giải pháp và hệ thống mạng cho nhiều nhà cung cấp dịch vụ (Service Provider), các doanh nghiệp lớn (Enterprise) và các doanh nghiệp nhỏ-và-vừa (Small - Medium Business) tại Việt nam từ năm 1997 khi ông làm việc cho tập đoàn Equant-SITA (nay là Orange Business Solution thuộc tập đoàn France Telecom).

Ông Sơn gia nhập Cisco đầu năm 2000 với vai trò kỹ sư tư vấn hệ thống. Năm 2003 ông được bổ nhiệm làm Giám đốc Kỹ thuật - Công nghệ Công ty Cisco Systems Việt nam. Từ năm 2007, ông đảm nhiệm vai trò Giám đốc Công nghệ (CTO) và Điều hành (COO) của Cisco Việt nam. Với gần 10 năm làm việc tại Cisco, trách nhiệm chính hiện nay của ông là định hướng chiến lược kinh doanh và phát triển nguồn lực công nghệ cho Cisco Việt nam và đối tác; phát triển thị trường và xúc tiến các giải pháp và công nghệ mạng thế hệ mới của Cisco tại Việt nam bao gồm: Advanced Technologies, Emerging Technologies, Data Center và Smart+Connected Communities. Trong vai trò COO, ông chịu trách nhiệm hỗ trợ CEO của Cisco Việt nam trong việc triển khai hiệu quả các quy trình và chương trình trong kiến trúc doanh nghiệp Cisco (Enterprise Architecture) cũng như xây dựng chiến lược phát triển dài hạn của Cisco tại Việt nam. Trong vai trò này, ông làm việc rất chặt chẽ với Cisco IT trong việc dùng thế mạnh Cisco IT triển khai các chiến lược kinh doanh, nâng cao năng suất lao động và tạo tiền đề cho sự cách tân (innovation) trong Cisco Việt nam cũng như phổ biến kinh nghiệm triển khai Cisco IT qua chương trình Cisco IT@Work cho khách hàng và đối tác tại Việt nam. Ông được giao làm đại diện cho Cisco System Việt nam tham gia vào các hiệp hội trong ngành ICT Việt nam như Hội Tin học Việt nam – VAIP, Hội Tin học TP. HCM – HCA, ICT Partnership Club, Hiệp hội An toàn – Thông tin (VNISA).

Trước khi gia nhập Cisco Systems, ông làm Quản lý nhóm dịch vụ cao cấp (Professional Service Manager) của Equant-SITA Việt nam nơi ông tham gia vào các dự án xây dựng mạng Internet Việt nam (VNN) từ năm 1997. Trong 3 năm trước đó ông là kỹ sư ICT của Liên doanh Dầu khí Vietsovpetro với công việc hỗ trợ hệ thống IT, mạng truyền thông và hệ thống tự động hóa. Từ năm 1992 đến 1994 ông là kỹ sư hệ thống chính của TRADEVICO-IBC (là Business Partner đầu tiên của IBM tại Việt nam) nơi ông tham gia triển khai và hỗ trợ hệ thống IT cho Tổng cục thuế, Kho bạc và Bộ tài chính.

Ông Sơn tốt nghiệp Khoa Công nghệ thông tin của Đại học Bách khoa TP Hồ Chí Minh. Trước đó ông có hai năm rèn luyện trong môi trường Quân đội tại khoa Thông tin, Học viện Kỹ thuật Quân sự.

HỆ THỐNG QUẢN LÝ ATTT THEO ISO 27001:2005
CÁCH TIẾP CẬN VÀ ÁP DỤNG THỰC TẾ
(Ông Trịnh Tuấn Dũng, Giám đốc kiểm định công ty BVQI)

Hệ thống Quản lý An toàn Thông Tin (ISMS)
theo ISO 27001:2005
Cách tiếp cận & áp dụng thực tế

Trịnh Tuấn Dũng
GD Chứng nhận
Bureau Veritas Certification VN

TP. Hồ Chí Minh, Ngày An toàn Thông tin – 18 tháng 11 năm 2009

Nội dung



- 1. Nhu cầu thực tế & giới thiệu về bộ tiêu chuẩn Quốc tế về Hệ thống Quản lý An toàn Thông tin (ISMS)**
- 2. Các bước thực hiện ISO 27001:2005 – Cách tiếp cận áp dụng thực tế.**
- 3. Ích lợi**

NHU CẦU CẦN CÓ CỦA HT AN TOÀN THÔNG TIN

Nhu cầu cần có của tiêu chuẩn

- ♦ Trước những năm 1970, công nghệ ATTT => Chính phủ, Quân sự, hay Ngân hàng
- ♦ Internet và kinh doanh trên mạng "on-line", ATTT => nhận dạng, chứng thực, và quản lý người sử dụng...
- ♦ Pháp luật về Chữ ký điện tử tạo điều kiện cho việc phát triển e-business, e-commerce
- ♦ Mọi người cần niềm tin và thực hiện có hiệu lực => HTQL ATTT

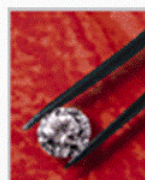


Bureau Veritas Certification Vietnam ISMS Security Day – 18 November 2009

4

Các HTQL nhằm cải tiến & cung cấp lòng tin

- ♦ Đảm bảo chất lượng sản phẩm & thoả mãn khách hàng => ISO 9001
- ♦ Bảo vệ môi trường sống cho cộng đồng → ISO 14001 ...
- ♦ Đảm bảo Sức khỏe, An toàn người lao động → OHSAS 18001
- ♦ Đảm bảo An toàn vệ sinh thực phẩm → ISO 22000
- ♦ Bảo mật thông tin liên lạc – là một loại tài sản đặc thù → ???
- ♦ HTQLATTT



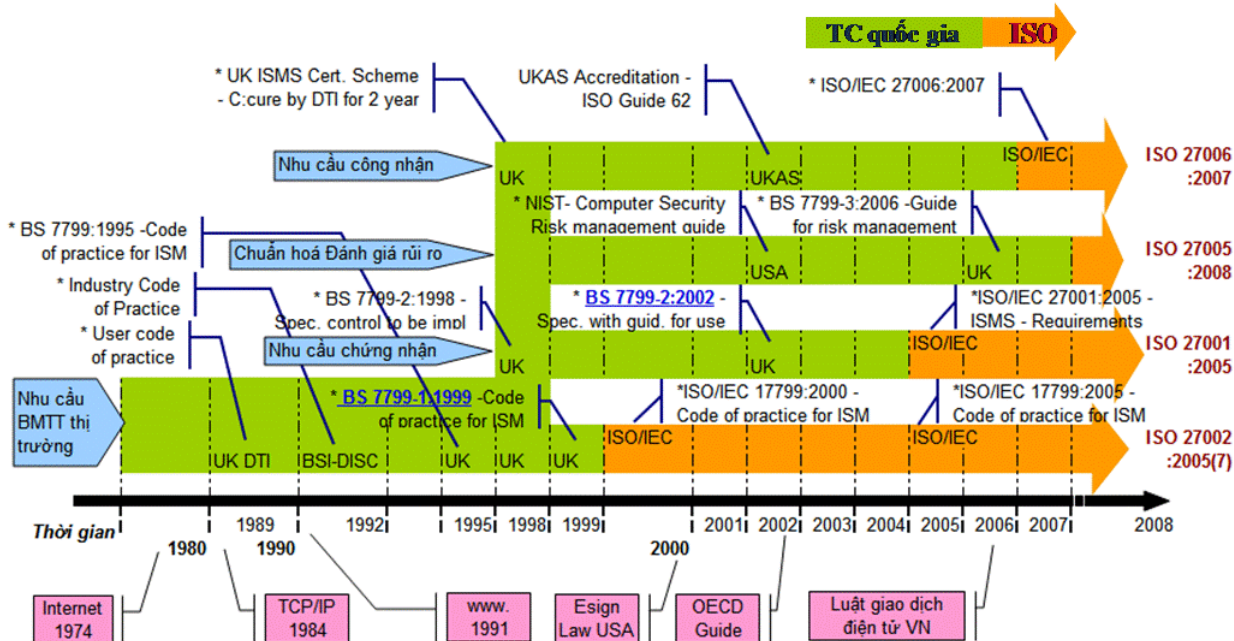
Bureau Veritas Certification Vietnam ISMS Security Day – 18 November 2009

5

Lịch sử của bộ tiêu chuẩn



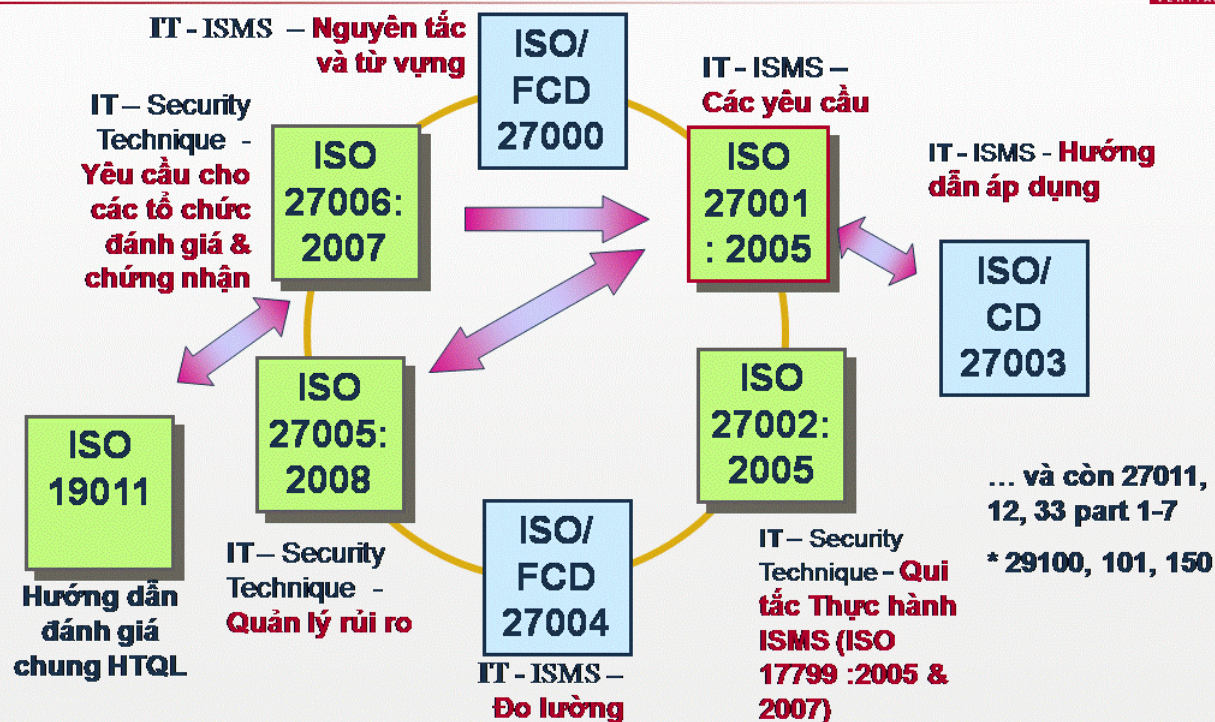
LỊCH SỬ PHÁT TRIỂN CỦA BỘ TIÊU CHUẨN ISO 27000:2005



Bureau Veritas Certification Vietnam ISMS Security Day – 18 November 2009

6

Bộ tiêu chuẩn ISO 27000 của JTC1 – SC 27



Bureau Veritas Certification Vietnam ISMS Security Day – 18 November 2009

7

Xu hướng phát triển của Bộ tiêu chuẩn ISO 27000



- ◆ Phát triển và hoàn thiện những tiêu chuẩn cơ bản: 27000 - Cơ sở, từ vựng, 27004 – Đo lường
- ◆ Phát triển và hoàn thiện những tiêu chuẩn Hướng dẫn (chung và đặc thù): 27003 – Áp dụng, 27007 – Đánh giá, 27011 – Telecommunication, 27012 – E Government, 27032 – Cybersecurity
- ◆ Đưa ra kỹ thuật bảo mật cho mạng – IT network: Bộ tiêu chuẩn 27033-1 cho tới 27033-7

JTC 1/SC 27- IT Security techniques

Standards and projects under the direct responsibility of JTC 1/SC 27 Secretariat

Sort Standard and/or project	Sort Current stage	Sort ICS
ISO/IEC FDIS 27011 Information technology – Information security management guidelines for telecommunications organizations based on ISO/IEC 27002	50.60	35.040
ISO/IEC NP 27012 Information technology - Security techniques – ISM guidelines for e-government services	10.99	35.040
ISO/IEC NP 27032 Guidelines for cybersecurity	10.99	35.040
ISO/IEC NP 27033 Information technology – IT Network security	10.99	35.040
ISO/IEC CD 27033-1 Information technology – Security techniques – IT network security – Part 1: Guidelines for network security	30.60	35.040
ISO/IEC WD 27033-2 Information technology – Security techniques – IT network security – Part 2: Guidelines for the design and implementation of network security	20.60	35.040
ISO/IEC WD 27033-3 Information technology – Security techniques – IT network security – Part 3: Reference networking scenarios – Risks, design techniques and control issues	20.60	35.040

Nguồn: ISO/JTC1/SC27

GIỚI THIỆU ISO 27001:2005 & CÁC BƯỚC ÁP DỤNG THỰC TẾ

Thông tin là gì?

Định nghĩa:

- **THÔNG TIN** là một loại tài sản, giống như những tài sản kinh doanh quan trọng khác, thông tin có giá trị đối với một tổ chức và do đó cần được **BẢO VỆ** một cách hợp lý. (ISO/IEC 17799:2000)

Thông tin có thể:



Bureau Veritas Certification Vietnam ISMS Security Day – 18 November 2009

10

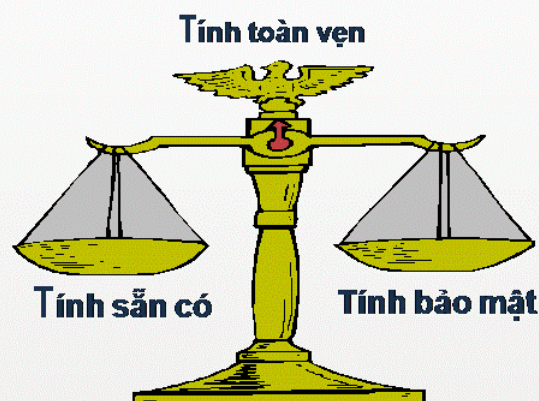
An toàn thông tin là gì?

CIA (Confidential-Integrity-Availability):

- **TÍNH BẢO MẬT:** Thông tin không sẵn có hoặc không nên để lộ cho cá nhân, tổ chức, đối tượng chưa được ủy quyền
- **TÍNH TOÀN VỆ:** Thông tin được bảo vệ và được giữ gìn trọn vẹn
- **TÍNH SẴN CÓ:** Luôn sẵn sàng và sẵn có sử dụng khi cần cho đối tượng đã được ủy quyền

(ISO/IEC 27001:2005 – Các yêu cầu)

Các tổ chức cần đạt được sự cân bằng...



“Sự duy trì các thuộc tính: tính bảo mật, tính toàn vẹn và tính sẵn có của thông tin; ngoài ra, các thuộc tính khác như tính xác thực, trách nhiệm giải trình, tính thừa nhận và tính đáng tin cậy cũng có thể liên quan”

Bureau Veritas Certification Vietnam ISMS Security Day – 18 November 2009

11

Hệ thống quản lý An toàn thông tin - ISMS là gì?



Định nghĩa:

"Hệ thống quản lý an toàn thông tin (ISMS) là một phần của hệ thống quản lý tổng thể, dựa trên cách tiếp cận theo rủi ro của kinh doanh, để thiết lập, thực hiện, điều hành, giám sát, xem xét, duy trì và cải tiến việc bảo mật thông tin"

Ghi chú: hệ thống quản lý bao gồm: cấu trúc của tổ chức, chính sách, các hoạt động hoạch định, trách nhiệm, việc thực hành, thủ tục, qui trình và nguồn lực."

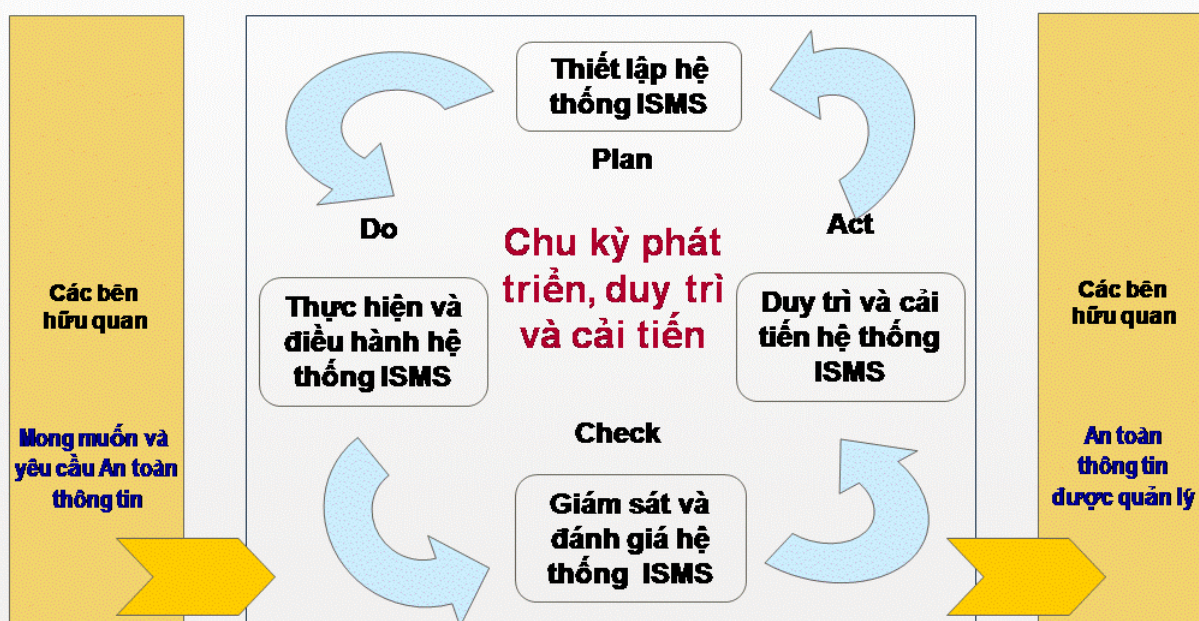
(ISO 27001:2005 cl 3.7)

Nhưng những lợi ích có được là gì?

Bureau Veritas Certification Vietnam ISMS Security Day – 18 November 2009

12

Giới thiệu ISO 27001:2005



Bureau Veritas Certification Vietnam ISMS Security Day – 18 November 2009

13

Giới thiệu ISO 27001:2005

► 4 Hệ thống quản lý an toàn thông tin

- 4.1 Các yêu cầu tổng quát
- 4.2 Thiết lập và quản lý hệ thống ISMS
- 4.3 Những yêu cầu về tài liệu

► 5 Trách nhiệm lãnh đạo

- 5.1 Cam kết của lãnh đạo
- 5.2 Quản lý các nguồn lực

► 6 Đánh giá nội bộ hệ thống ISMS

► 7 Xem xét lãnh đạo hệ thống ISMS

► 8 Việc cải tiến ISMS

- 8.1 Cải tiến thường xuyên
- 8.2 Hành động sửa chữa
- 8.3 Hành động phòng ngừa

Phụ lục A bao gồm :

- 11 phần:
 5. Chính sách ISMS
 6. Cơ cấu tổ chức ISMS
 7. Quản lý tài sản
 8. Bảo mật nguồn nhân lực
 9. Bảo mật môi trường vật lý
 10. Quản lý hoạt động và truyền thông
 11. Kiểm soát truy cập
 12. Thu nạp, duy trì và phát triển hệ thống thông tin
 13. Quản lý sự cố ISMS
 14. Duy trì liên tục hoạt động kinh doanh
 15. Tính tuân thủ

► 39 mục tiêu kiểm soát

► 132 biện pháp kiểm soát



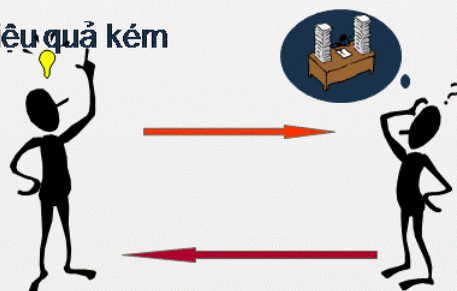
Bureau Veritas Certification Vietnam ISMS Security Day – 18 November 2009

14

ISMS theo ISO 27001:2005

Một số “vấn đề” có thể tồn tại của các HTQL vận hành theo tiêu chuẩn quốc tế ISO (9001, 14001, 22000...):

- ♦ Phức tạp nhiều hệ thống
- ♦ Tốn giấy, tốn công
- ♦ Hình thức, không thực tế
- ♦ Hiệu quả kém



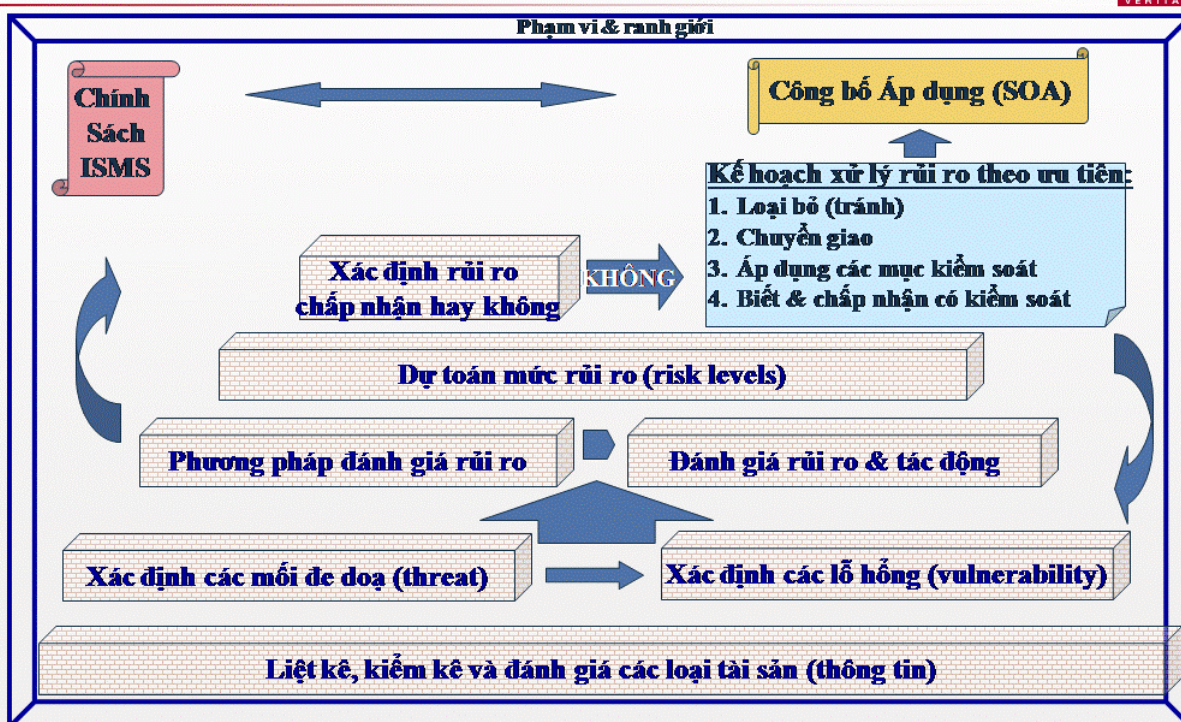
Tiêu chuẩn này chỉ rõ:

- ♦ Mục 0.1 Tổng quan “Áp dụng ISMS với mức độ tùy thuộc vào nhu cầu của tổ chức, nghĩa là tình huống đơn giản chỉ yêu cầu ISMS đơn giản”
- ♦ Mục 0.3 Tương thích với các HTQL khác: “Tiêu chuẩn quốc tế này hoàn toàn tương thích với ISO 9001:2000 và ISO 14001:2004 để hỗ trợ cho việc áp dụng và vận hành tích hợp. Một HTQL được thiết kế thích hợp có thể thỏa mãn tất cả các tiêu chuẩn này”
- ♦ Mục 1.2 Áp dụng / Chú thích: “Dùng HTQL hiện có để thỏa mãn các yêu cầu của tiêu chuẩn này sẽ tốt hơn trong đa số các trường hợp”

Bureau Veritas Certification Vietnam ISMS Security Day – 18 November 2009

15

Xây dựng ISMS theo ISO 27001:2005



Bureau Veritas Certification Vietnam ISMS Security Day – 18 November 2009

16

SO SÁNH VỚI HTQL HIỆN CÓ (ISO 9001:2008)



ISO 27001:2005

HTQL hiện có (hay ISO 9001:2008)

► 4 Hệ thống quản lý an toàn thông tin

- 4.1 Các yêu cầu tổng quát
- 4.2 Thiết lập và quản lý hệ thống ISMS
- 4.3 Những yêu cầu về tài liệu

► 5 Trách nhiệm lãnh đạo

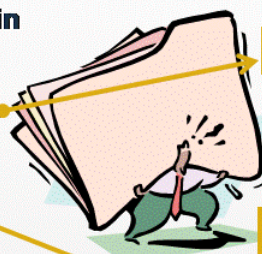
- 5.1 Cam kết của lãnh đạo
- 5.2 Quản lý các nguồn lực

► 6 Đánh giá nội bộ hệ thống ISMS

► 7 Xem xét lãnh đạo hệ thống ISMS

► 8 Việc cải tiến ISMS

- 8.1 Cải tiến thường xuyên
- 8.2 Hành động sửa chữa
- 8.3 Hành động phòng ngừa



Xem trang trước

Bảng so sánh tương đồng giữa 9001/14001&27001:

4.2.3 & 4.2.4
5.1 & 5.2
6.2
8.2.2
5.6
8.5.1
8.5.2
8.5.3

Bureau Veritas Certification Vietnam ISMS Security Day – 18 November 2009

17

Giới thiệu ISO 27001:2005



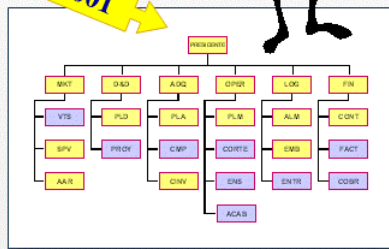
Phụ lục A bao gồm :

- ▶ **11 phần:**
- 5. Chính sách ISMS
- 6. Cơ cấu tổ chức ISMS
- 7. Quản lý tài sản
- 8. Bảo mật nguồn nhân lực
- 9. Bảo mật môi trường vật lý
- 10. Quản lý hoạt động và truyền thông
- 11. Kiểm soát truy cập
- 12. Thu nạp, duy trì và phát triển hệ thống thông tin
- 13. Quản lý sự cố ISMS
- 14. Duy trì liên tục hoạt động kinh doanh
- 15. Tính tuân thủ
- ▶ **39 mục tiêu kiểm soát**
- ▶ **132 biện pháp Kiểm soát**

Giống ISO 9001

Tương tự ISO 9001

Mối so với ISO 9001 nhưng bài bản



Các tổ chức chuyên môn



Khách hàng



Các bên cung cấp thứ Ba

Kiểm kê – Có chủ - Phân loại – Nhãn - QĐ sử dụng

Bureau Veritas Certification Vietnam ISMS Security Day – 18 November 2009

18

Giới thiệu ISO 27001:2005



Phụ lục A bao gồm :

- ▶ **11 phần:**
- 5. Chính sách ISMS
- 6. Cơ cấu tổ chức ISMS
- 7. Quản lý tài sản
- 8. Bảo mật nguồn nhân lực
- 9. Bảo mật môi trường vật lý
- 10. Quản lý hoạt động và truyền thông
- 11. Kiểm soát truy cập
- 12. Thu nạp, duy trì và phát triển hệ thống thông tin
- 13. Quản lý sự cố ISMS
- 14. Duy trì liên tục hoạt động kinh doanh
- 15. Tính tuân thủ
- ▶ **39 mục tiêu kiểm soát**
- ▶ **132 biện pháp Kiểm soát**

Nhân viên/nhà thầu/bên thứ 3 – trước/trong/sau HĐ

Tương tự ISO 9001

Tương tự ISO 9001



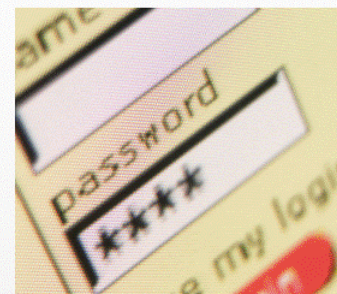
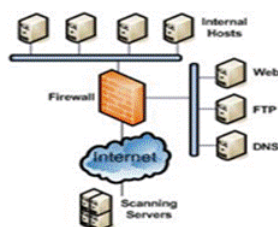
Bureau Veritas Certification Vietnam ISMS Security Day – 18 November 2009

19

Giới thiệu ISO 27001:2005

Phụ lục A bao gồm :

- ▶ **11 phần:**
 - 5. Chính sách ISMS
 - 6. Cơ cấu tổ chức ISMS
 - 7. Quản lý tài sản
 - 8. Bảo mật nguồn nhân lực
 - 9. Bảo mật môi trường vật lý
 - 10. Quản lý hoạt động và truyền thông
 - 11. Kiểm soát truy cập
 - 12. Thu nạp, duy trì và phát triển hệ thống thông tin
 - 13. Quản lý sự cố ISMS
 - 14. Duy trì liên tục hoạt động kinh doanh
 - 15. Tính tuân thủ
- ▶ **39 mục tiêu kiểm soát**
- ▶ **132 biện pháp Kiểm soát**



Bureau Veritas Certification Vietnam ISMS Security Day – 18 November 2009

20

ÍCH LỢI

Lợi ích của an toàn thông tin

♦ Bảo vệ tài sản thông tin một cách thích hợp

- ♦ Kiểm soát dựa trên rủi ro
- ♦ Không bị Thiếu / Thừa

♦ Lợi thế cạnh tranh

♦ Sự tuân thủ pháp luật

♦ Hình ảnh

♦ Lợi nhuận



♦ Thành lập nền tảng vững chắc cho chính sách bảo mật thông tin

♦ Là bằng chứng thấy được về những thực hành được áp dụng cho các bên quan tâm:

- ♦ Các khách hàng thương mại
- ♦ Khách hàng là người sử dụng cuối cùng
- ♦ Đối với nhân viên (kiểm toán)
- ♦ Đối với các cơ quan quản lý

BUREAU VERITAS CERTIFICATION VIETNAM

▶ Phát hành 2000 Giấy chứng nhận phù hợp với các tiêu chuẩn quốc tế cho các HTQL

▶ Phù hợp ISO 17021:2006 & được chuyển thành Trung tâm chứng nhận (ICC) từ tháng 9 năm 2008

- Quyết định chứng nhận với công nhận của UKAS & ANAB.
- Kịp thời hơn với nhu cầu khách hàng

▶ Có chuyên gia đánh giá người Việt Nam

▶ Khách hàng tiêu biểu tại Việt Nam ISO 27001:2005—UKAS công nhận

- YKK.
- BKIS





**BUREAU
VERITAS**

Move Forward with Confidence

Để biết thêm thông tin, vui lòng liên hệ: **Ms. Mỹ Hạnh**

Tel.: 3812 2196 Ext. 130 or E-mail: my-hanh.nguyen@vn.bureauveritas.com

Thank you!

SESSION 1: ATTT MẠNG VÀ HỆ THỐNG

Nội dung:

1. Giải pháp chống thất thoát dữ liệu cho doanh nghiệp
2. Đảm bảo tính liên tục của doanh nghiệp và khôi phục sau thảm họa
3. Thảo luận + Bốc thăm trúng thưởng

Người điều phối:



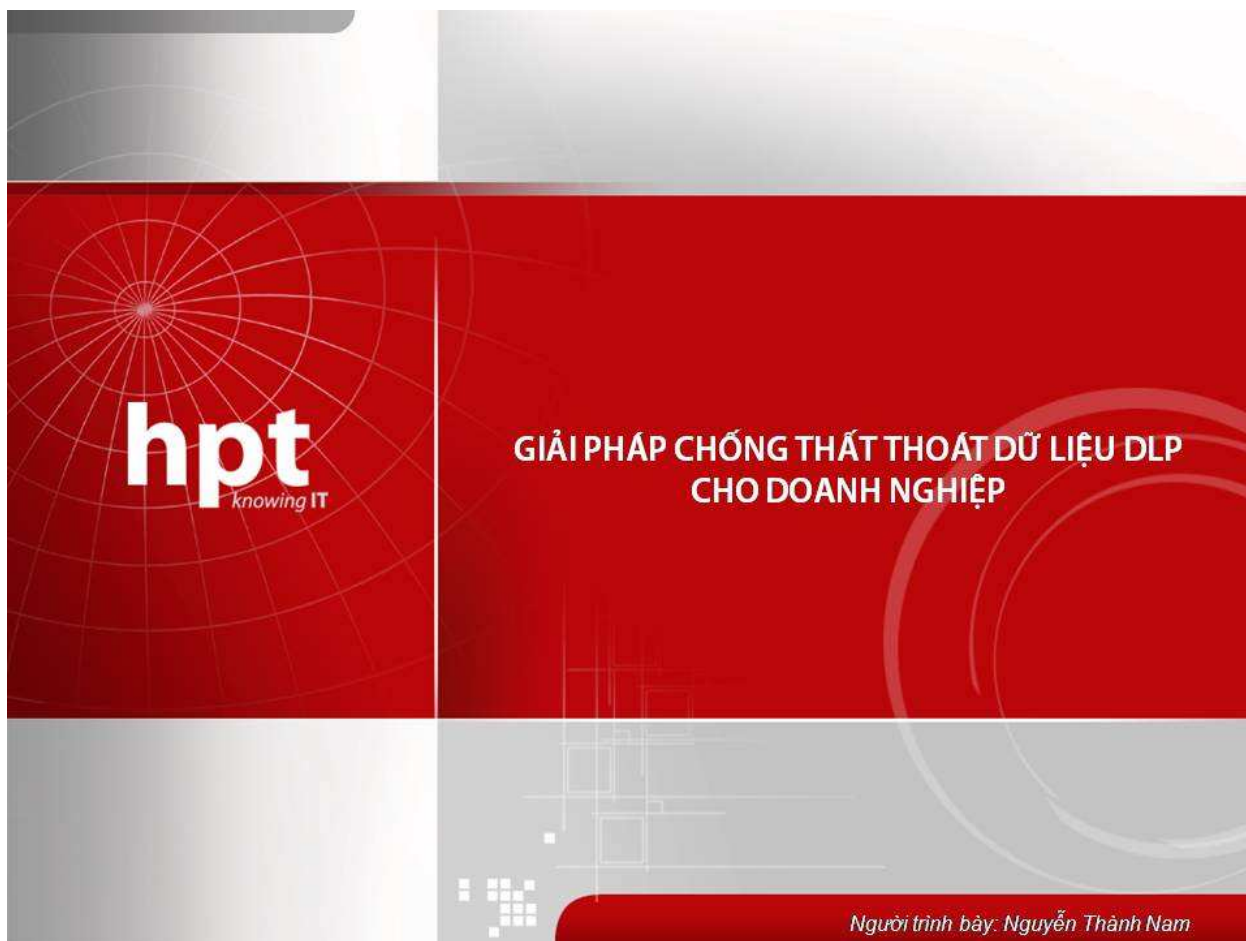
Ông Phùng Hải

CISSP- Trưởng ban an toàn mạng và hệ thống Chi hội VNISA phía Nam. Giám đốc phát triển kinh doanh công ty Misoft HCM.

Ông Phùng Hải tốt nghiệp cử nhân tại Úc và có trên 10 năm kinh nghiệm trong lĩnh vực ATTT

GIẢI PHÁP CHỐNG THẤT THOÁT DỮ LIỆU CHO DOANH NGHIỆP

(Ông Nguyễn Thành Nam, chuyên gia bảo mật công ty HPT)





NỘI DUNG

1. Những thách thức trong bảo mật dữ liệu
2. Mô hình phân loại dữ liệu
3. Giải pháp chống thất thoát dữ liệu DLP
4. Ứng dụng DLP & Những lợi ích
5. Thị trường giải pháp DLP

HPT VIETNAM CORPORATION
HPT VIETNAM CORPORATION



1. Những thách thức trong bảo mật dữ liệu

knowing IT

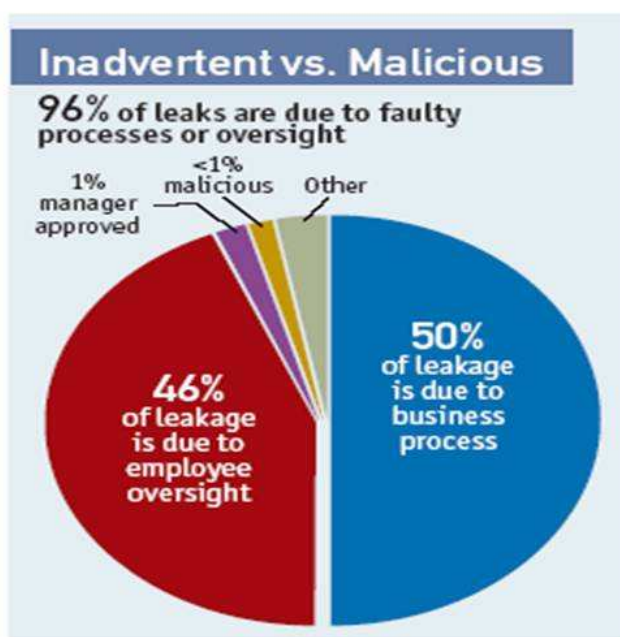
Những thách thức trong bảo mật dữ liệu



Tồn tại nhiều loại dữ liệu trong thế giới của chúng ta:

- **Trong Công nghệ thông tin:** Mã nguồn, Chính sách bảo mật, Kiến trúc hệ thống IT
- **Trong ngành Sản xuất:** công thức sản phẩm, chiến lược phát triển
- **Trong ngành Y tế:** thông tin bệnh nhân
- **Trong Tài chính/ Ngân hàng:** Dữ liệu khách hàng, Dữ liệu nhân viên
- **Trong ngành Bảo hiểm:** Dữ liệu khách hàng, Kế hoạch kinh doanh của các đơn vị
- .V.V.

Những thách thức trong bảo mật dữ liệu



Nguồn: Vontu Assessment Risk

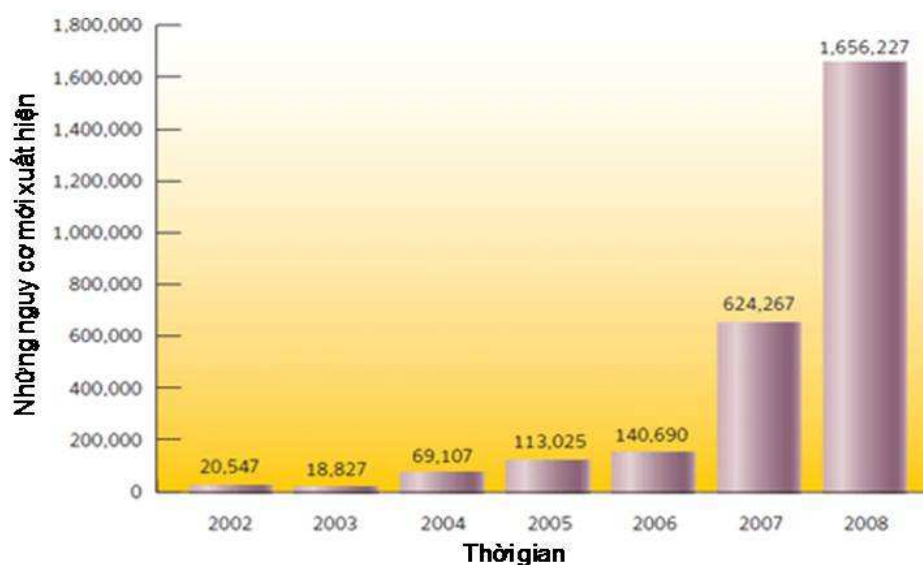


Những thách thức trong bảo mật dữ liệu



Những thách thức trong bảo mật dữ liệu

Các loại mã độc mới xuất hiện



Nguồn: Vontu Assessment Risk



Những thách thức trong bảo mật dữ liệu

850,000 – Tại tập đoàn bảo hiểm Blue Cross Blue Shield, thông tin bác sĩ bị mất gồm họ tên, địa chỉ và cả mã số thuế, khi một chiếc máy tính xách tay lưu trữ các thông tin này bị lấy trộm.

700,000 – 1 năm kể từ khi bị đột nhập, Công ty quản lý dược phẩm cho biết đã có khoảng 700,000 dữ liệu bị tiết lộ & Công ty đang đưa ra mức thưởng 1 triệu USD cho người cung cấp thông tin bắt giữ kẻ đột nhập.



BlueCross BlueShield Association



EXPRESS SCRIPTS®

(Nguồn: Dayton Bussiness Journal – 10/2009)

(Nguồn: IDG News Service – 09/2009)



Những thách thức trong bảo mật dữ liệu

2 – Đã có 2 vụ mất dữ liệu tại Công ty sản xuất Dupont, Công ty đã kiện một nhân viên cũ vì đã cố tình lén mang những bí mật kinh doanh bán cho Trung Quốc và các đối thủ cạnh tranh.

500,000 – Công ty Network Solutions đã thông báo về việc thất thoát thông tin của hơn 500,000 thẻ khách hàng sau khi hệ thống bị đột nhập & Công ty đã phải mất hàng triệu USD để khắc phục những thiệt hại



The miracles of science™



(Nguồn: Dayton Bussiness Journal – 10/2009)

(Nguồn: IDG News Service – 09/2009)

Những thách thức trong bảo mật dữ liệu



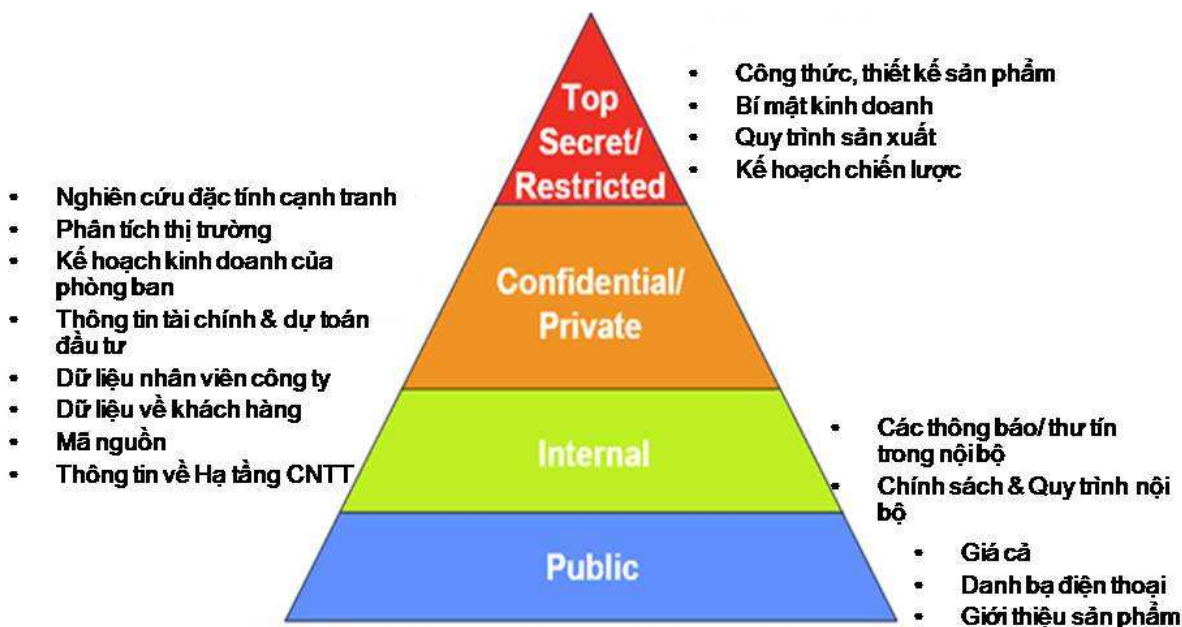
Sắp xếp dữ liệu ?

Chống thất thoát dữ liệu ?

1. Ai đang sử dụng những dữ liệu nhạy cảm ?
2. Phương án bảo vệ những dữ liệu nhạy cảm không bị thất thoát ?
3. Phương án xây dựng các chính sách phù hợp nhằm bảo vệ dữ liệu ?
4. Phương án để giám sát các phiên truyền gửi dữ liệu của người dùng cuối ?
5. Phương án cần thiết để biết người dùng cuối đang cố vượt qua các chính sách của hệ thống ?
6. Có bao nhiêu thư điện tử vi phạm quy định bảo mật ?
7. Phương án giám sát các dữ liệu thất thoát qua đường Web hay Instant Messenger ?

2. Mô hình phân loại dữ liệu

knowing IT



Các bước để có một hệ thống bảo mật dữ liệu:

1. Xác định & Sắp xếp dữ liệu
2. Đặt độ ưu tiên cho các đối tượng cần bảo mật
3. Thiết lập các chính sách bảo mật thống nhất
4. Lựa chọn & Triển khai giải pháp chống thất thoát dữ liệu
5. Xây dựng các tài liệu, ý thức & đào tạo
6. Xác lập về quyền sở hữu & trách nhiệm rõ ràng
7. Tự động áp đặt các chính sách
8. Đo lường & Giám sát





3. Giải pháp chống thất thoát dữ liệu DLP

knowing IT



Giải pháp chống thất thoát dữ liệu DLP

Nơi lưu trữ những dữ liệu cần bảo mật của bạn?



Những dữ liệu bảo mật được sử dụng như thế nào?



Cách nào tốt nhất để ngăn chặn các dữ liệu bị thất thoát ra ngoài?



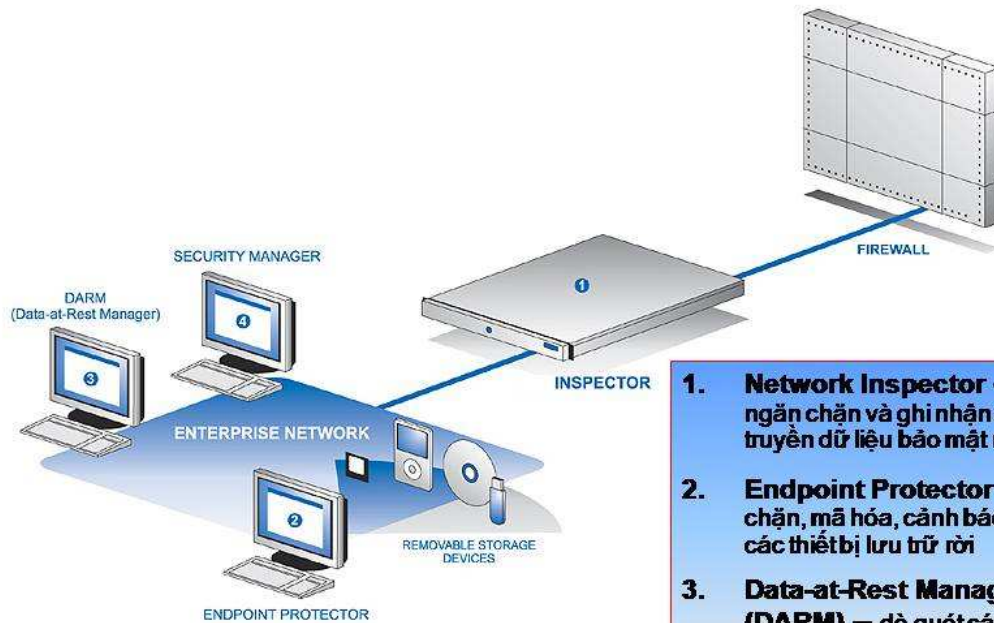
PHÁT HIỆN

GIÁM SÁT

BẢO VỆ

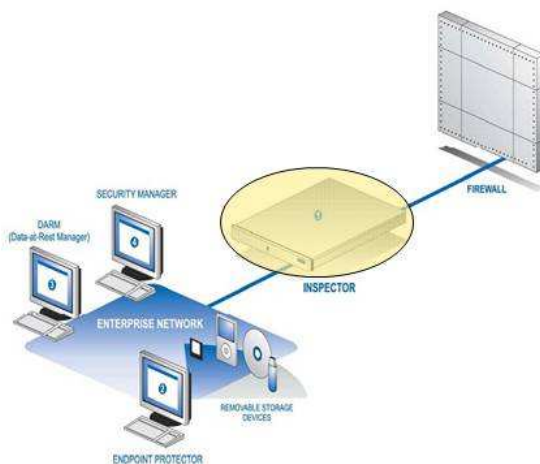
PHÒNG CHỐNG THẤT THOÁT DỮ LIỆU

Giải pháp chống thất thoát dữ liệu DLP



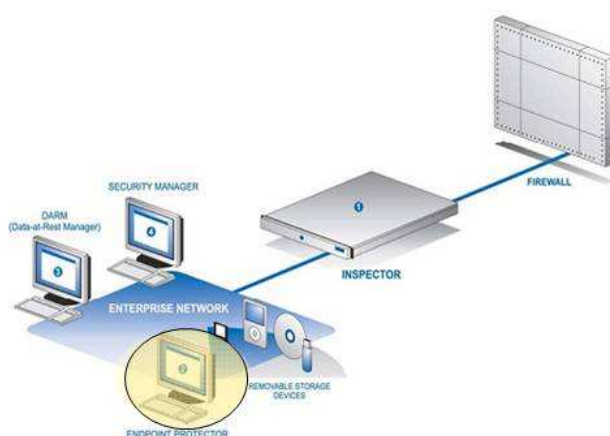
1. **Network Inspector** – giám sát, ngăn chặn và ghi nhận các phiên truyền dữ liệu bảo mật ra ngoài
2. **Endpoint Protector** – ngăn chặn, mã hóa, cảnh báo và kiểm tra các thiết bị lưu trữ rời
3. **Data-at-Rest Manager (DARM)** – dò quét các dữ liệu bảo mật trên mạng
4. **Security Manager** – xác định, lấy mẫu và giám sát tập trung các dữ liệu bảo mật

Thành phần Network Inspector



1. **Bảo vệ các giao thức**
 - SMTP, POP3
 - HTTP, FTP
 - HTTPS, SSL
 - Instant Messenger (YM, AOL, Skype, ...)
 - Các ứng dụng P2P
2. **Độ chính xác**
 - Không có tình trạng báo động giả
 - Tỷ lệ phát hiện cao
 - Linh động đối với các thao tác trên dữ liệu: Trích xuất dữ liệu, Chuyển đổi hồ sơ, Nén dữ liệu, Nhúng dữ liệu, Thay đổi cách thể hiện dữ liệu (12-13-14, 12 13 14)
3. **Báo cáo**
 - Báo cáo dạng bảng chi tiết
 - Trích xuất báo cáo theo định dạng MS

Thành phần Endpoint Protector



1. Giám sát truy cập

- Người dùng cá nhân
- Nhóm người dùng/ Nhóm máy tính
- Các loại thiết bị
- Các loại hồ sơ

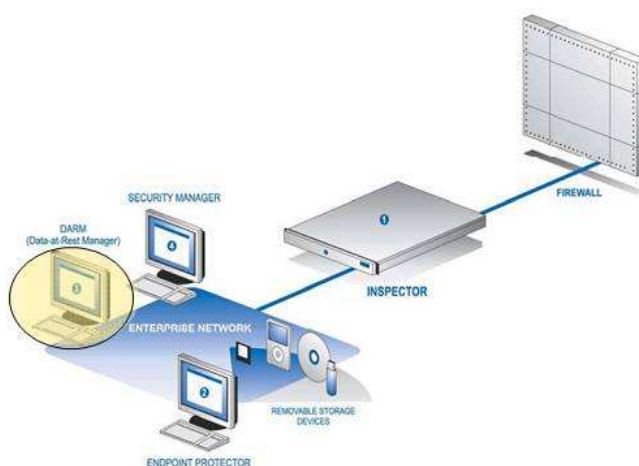
2. Các tính năng

- Tích hợp LDAP
- Mã hóa hồ sơ
- Kiểm tra phần cứng
- Kiểm soát hồ sơ
- Phương thức Online/Offline

3. Báo cáo

- Báo cáo dạng bảng chi tiết
- Trích xuất báo cáo theo định dạng MS

Thành phần Data-at-rest Manager

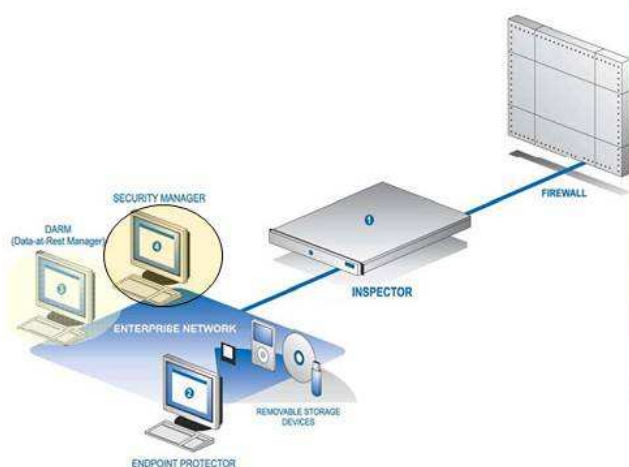


1. Các tính năng

- Phát hiện các dữ liệu bảo mật được lưu trữ không đúng vị trí
- Sắp xếp dữ liệu
- Hỗ trợ các thành phần tìm kiếm dữ liệu dạng ký tự hay nhị phân
- Dò quét các hồ sơ cục bộ và trên hệ thống mạng
- Dò quét các hồ sơ trong các phương tiện lưu trữ di động

2. Báo cáo

- Báo cáo dạng bảng chi tiết
- Trích xuất báo cáo theo định dạng MS



1. Các tính năng

- Xác định các chính sách thống nhất cho doanh nghiệp
- Sửa chữa và báo cáo về các sự cố
- Phát hiện chính xác các dữ liệu nhạy cảm trên hệ thống

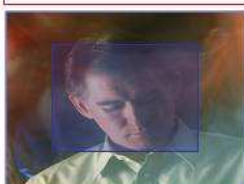
2. Báo cáo

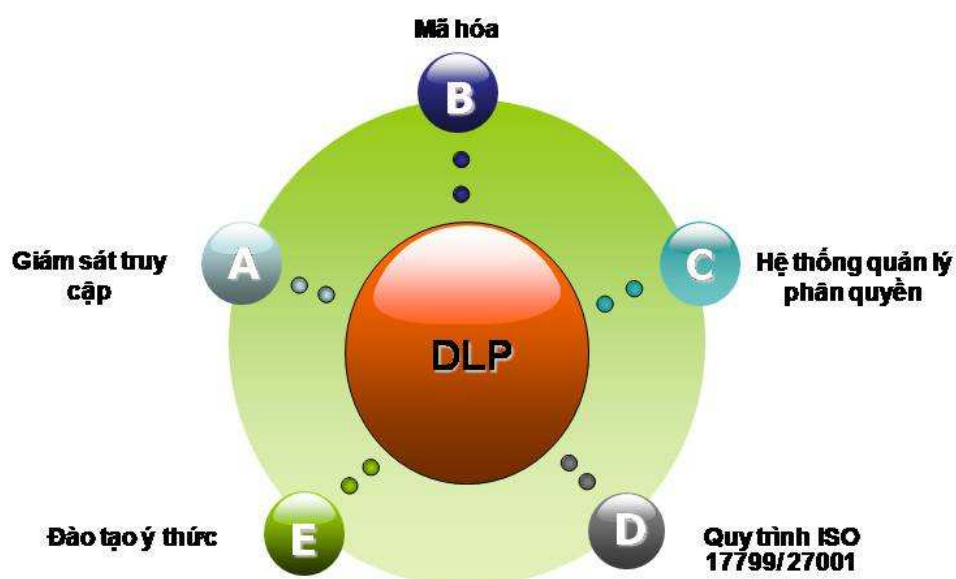
- Báo cáo dạng bảng chi tiết
- Trích xuất báo cáo theo định dạng MS



8+1 yếu tố cơ bản cho giải pháp Chống thất thoát dữ liệu

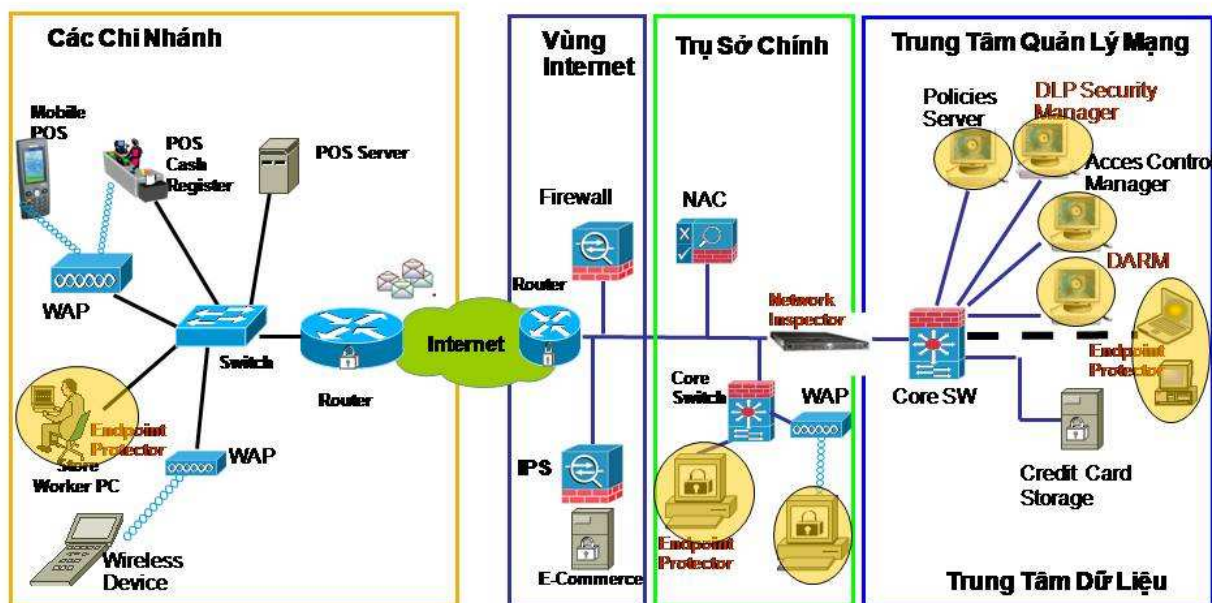
1. Không nên sử dụng phần mềm, nên dùng dạng phần cứng
2. Tính bảo mật
3. Bao hàm tất cả các kênh truyền dữ liệu
4. Tính chính xác (Tỷ lệ báo động giả tối thiểu)
5. Linh hoạt đối với những thao tác trên dữ liệu
6. Bao hàm tất cả các nguồn và định dạng của dữ liệu
7. Các nội dung và kênh truyền đã được mã hóa
8. Quản lý các dữ liệu "at Rest" – eDiscovery
9. Bảo vệ đầu cuối





4. Ứng dụng DLP & Những lợi ích

knowing IT





Ngăn chặn người dùng cuối gửi các dữ liệu bảo mật ra ngoài

6



Phát hiện và ngăn chặn các sự cố về dữ liệu

7



Cảnh báo cho người dùng, nhân viên

8



Hình thành các tiến trình tự động sửa chữa

9



Các chính sách bảo mật dữ liệu được quản lý tập trung

10



PHÁT HIỆN

- Xác định vị trí lưu trữ của dữ liệu
- Tạo các vùng lưu trữ cho các dữ liệu nhạy cảm
- Quản lý các dữ liệu rõ ràng



GIÁM SÁT

- Cách thức dữ liệu được sử dụng trong hệ thống
- Hiểu rõ về nội dung và ngữ cảnh sử dụng dữ liệu
- Ghi nhận được những vi phạm chính sách



BẢO VỆ

- Chủ động bảo mật các dữ liệu
- Ngăn chặn thất thoát các dữ liệu bảo mật
- Áp đặt các chính sách bảo vệ dữ liệu



QUẢN LÝ

- Xác định các chính sách bảo mật dữ liệu thống nhất cho doanh nghiệp
- Sửa chữa và báo cáo các sự cố về dữ liệu
- Phát hiện chính xác các nội dung

Four Categories for Potential Business Value from IT Security		
More Difficult to Quantify	Manage Risk	Enhance Revenue
Easier to Quantify	Achieve and Sustain Compliance	Reduce Cost
	Stronger Technical Orientation	Stronger Business Orientation

Nguồn: Aberdeen Group – 06/2009

5. Thị trường giải pháp DLP

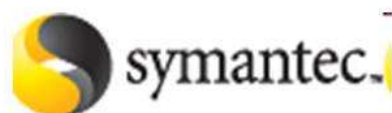
knowing IT



Safend – Nhà cung cấp giải pháp bảo mật đầu cuối hàng đầu, cho phép các doanh nghiệp bảo mật thông tin trong môi trường di động – từ máy tính xách tay, thiết bị lưu trữ di động và các giao thức truyền tải không dây đến các thiết bị di động thông minh – nâng cao hiệu suất làm việc mà không cần lưu tâm vấn đề bảo mật.



GTB Technologies – Bộ giải pháp của GTB khác biệt so với những đối thủ cạnh tranh, nhắm vào các nguy cơ từ những người dùng không tin cậy và cả những người dùng tin cậy. Với tính năng lấy mẫu, giải pháp có thể dò quét tất cả các giao thức theo thời gian thực và cho phép ngăn chặn thất thoát dữ liệu ngay lập tức, cũng như tạo ra các báo cáo.



Symantec – Symantec giúp khách hàng và doanh nghiệp bảo mật và quản lý các thông tin. Phần mềm và dịch vụ của Symantec cho phép bảo vệ các thông tin bảo mật hiệu quả và hoàn chỉnh trước các nguy cơ bất kể các dữ liệu được lưu trữ ở đâu và sử dụng như thế nào.

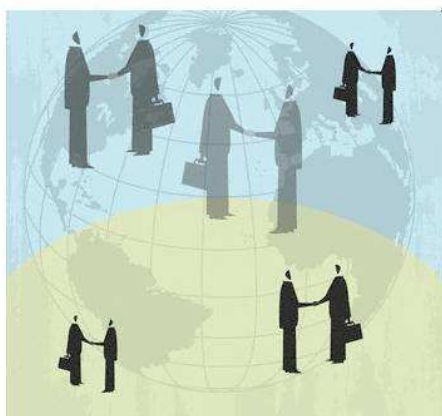


RSA – Bộ sản phẩm phòng chống thất thoát dữ liệu cung cấp một hướng bảo mật dựa theo các chính sách để bảo vệ dữ liệu, cho phép khách hàng sắp xếp các dữ liệu nhạy cảm, phát hiện các phiên truyền gửi dữ liệu trong doanh nghiệp, áp đặt các điều khiển, báo cáo và kiểm tra để bảo đảm tính tuân thủ các chính sách.

hpt
knowing IT

Thị trường giải pháp DLP

hpt
knowing IT



safend
Securing Your Endpoints

GTB Technologies
Next Generation DLP

RSA

The Security Division of EMC

McAfee
SECURITY

symantec

TREND
MICRO



Cám ơn!

hpt
knowing IT

knowing IT

Am tường công nghệ - Thấu hiểu thông tin

ĐẢM BẢO TÍNH LIÊN TỤC CỦA DOANH NGHIỆP VÀ KHÔI PHỤC SAU THẢM HỌA

(Ông Đỗ Ngọc Huy, chuyên gia bảo mật công ty FPT)

ĐẢM BẢO TÍNH LIÊN TỤC CHO DOANH NGHIỆP VÀ KHÔI PHỤC THẢM HỌA

Trình bày: Đỗ Ngọc Huy
FPT Information System
CCIE Security #16931

Nội dung

- Đánh giá tình hình triển khai khôi phục thảm họa
- Sơ lược về xây dựng kế hoạch đảm bảo tính liên tục và khôi phục thảm họa

ĐÁNH GIÁ TÌNH HÌNH TRIỂN KHAI KHÔI PHỤC THẢM HỌA

Khảo sát về khôi phục thảm họa trên thế giới

- Ngân sách chi tiêu cho Khôi phục thảm họa có tăng lên trong năm 2009.
- Mục tiêu về thời gian khôi phục đã giảm xuống còn 4 giờ trong năm 2009
- 25% thử nghiệm là không đạt yêu cầu
- Chi phí trung bình cho việc triển khai các kế hoạch Khôi phục thảm họa cho mỗi sự cố ngưng trệ hệ thống trên toàn thế giới là 287.600 USD
- Tại khu vực Bắc Mỹ, chi phí cho các tổ chức tài chính thực hiện việc Khôi phục thảm họa là 650.000 USD.

Nguồn: Symantec

Khảo sát về khôi phục thảm họa trên thế giới (tt)

- Một phần tư số các thử nghiệm khôi phục thảm họa là không thành công
- Mất trung bình khoảng 3 tiếng để kích hoạt lại các hoạt động chính sau một sự cố mất điện
- Mất đến 4 tiếng mới có thể hồi phục trở lại và vận hành bình thường
- Nhân sự vận hành gấp đôi so với năm ngoái
- 70% đơn vị khảo sát cho biết Ủy ban Khôi phục sau thảm họa của họ bao gồm cả Giám đốc thông tin (CIO), Giám đốc công nghệ (CTO) và Trưởng phòng CNTT
- 60% các ứng dụng được cho là không thể thiếu

Nguồn: Symantec

Khảo sát về khôi phục thảm họa trên thế giới (tt)

- Những lý do khiến cho các tổ chức không tiến hành thử nghiệm bao gồm
 - Thiếu các nguồn lực do quỹ thời gian của nhân sự không nhiều (48%)
 - Gây ngừng trệ hoạt động của nhân viên (44%)
 - Vấn đề chi phí (44%)
 - Gây ngừng trệ tới hoạt động của khách hàng (40%)

Nguồn: Symantec

Khảo sát về khôi phục thảm họa trên thế giới (tt)

- Ảo hoá vẫn là một thách thức lớn
 - Khoảng 64% các đơn vị khảo sát cho biết ảo hoá đang khiến họ phải đánh giá lại những kế hoạch khôi phục thảm họa
 - Hơn một nửa số đơn vị khảo sát trên toàn cầu đã thừa nhận:
 - Sự thiếu thốn các công cụ quản lý lưu trữ là thách thức lớn nhất trong việc bảo vệ dữ liệu và những ứng dụng quan trọng trong môi trường ảo (53%).
 - Sự hạn hẹp về tài nguyên như con người, ngân sách và không gian là những thách thức lớn trong việc sao lưu máy ảo. (51%).

Nguồn: Symantec

Khảo sát về khôi phục thảm họa tại Việt Nam

- Có khoảng cách rất lớn giữa nhận thức của các Doanh Nghiệp vừa và nhỏ (DNVVN) về việc sẵn sàng ứng phó thảm họa và thực tế chuẩn bị
- 82% các đơn vị, tổ chức được khảo sát cho biết hài lòng ở một mức độ nào đó/hoặc rất hài lòng với những kế hoạch ứng phó thảm họa hiện có
- 84% cho biết cảm thấy được bảo vệ tốt/hoặc ở mức độ vừa phải trong trường hợp có thảm họa xảy ra
- Trung bình, các DNVVN được khảo sát gặp phải sự cố ngưng trệ hoạt động 3 lần trong vòng 12 tháng.

Nguồn: Symantec

Khảo sát về khôi phục thảm họa tại Việt Nam (tt)

- Khoảng 1/5 các DNVVN (chiếm 23%) thực hiện sao lưu dữ liệu hàng ngày.
- Một DNVVN trung bình chỉ sao lưu khoảng 60% dữ liệu công ty và dữ liệu khách hàng
- Hơn một nửa các DNVVN dự tính họ sẽ mất khoảng 40% dữ liệu của mình nếu hệ thống điện toán của họ bị phá hủy trong hỏa hoạn.
- Ước tính chi phí cho việc ngưng trệ hệ thống trung bình là 15,000 USD mỗi ngày

Nguồn: Symantec

SƠ LƯỢC VỀ XÂY DỰNG KẾ HOẠCH ĐẢM BẢO TÍNH LIÊN TỤC VÀ KHÔI PHỤC THẢM HỌA

Giai đoạn khởi tạo dự án

- Thiết lập quản lý
- Thiết lập sự cần thiết của kế hoạch
- Định nghĩa phạm vi của dự án và mục tiêu
- Thành lập đội ngũ
- Xác định nhiệm vụ
- Lên kế hoạch cho các buổi họp và thời gian thực hiện
- Xác định sự cần thiết của những công cụ thu thập dữ liệu tự động
- Trình bày báo cáo ban đầu cho nhà quản lý

Xác định vai trò

- Đội ngũ quản lý thực thi cấp cao
- Đội ngũ quản lý chức năng cấp cao
- Ủy ban đảm bảo tính liên tục và khôi phục

Phân tích tác động đến doanh nghiệp (BIA)

- Mục đích của BIA là nhằm cung cấp cho doanh nghiệp sự hiểu biết những tác động của sự kiện làm gián đoạn hoạt động của doanh nghiệp.
- Tác động có thể mang tính định tính
- Tác động có thể mang tính định lượng
- Đánh giá lỗ hổng bảo mật là một phần của BIA

3 mục tiêu chính của BIA

- Sắp xếp độ ưu tiên theo tính chất quan trọng
- Ước lượng thời gian gián đoạn
- Yêu cầu tài nguyên

8 bước thực hiện BIA

- Chọn ứng viên phỏng vấn để thu thập dữ liệu
- Xác định kỹ thuật thu thập dữ liệu
- Phát triển bảng câu hỏi
 - Định tính
 - Định lượng
- Phân tích dữ liệu được thu thập
- Xác định những hệ thống quan trọng trong doanh nghiệp

8 bước thực hiện BIA (tt)

- Tính toán thời gian gián đoạn tối đa chịu đựng được (MTD) cho từng thành phần quan trọng
- Xây dựng tính ưu tiên những thành phần quan trọng dựa trên MTD
- Lập tài liệu những vấn đề tìm thấy và cung cấp cho quan lý, cùng với những đề xuất

Những hiểm họa tiềm tàng

- Thảm họa tự nhiên
 - Thức ăn
 - Bão
 - Động đất
 - Lũ lụt
- Những sự kiện do con người
 - Khủng bố
 - Hỏa hoạn
 - Sai lầm trong vận hành
- Thảm họa kỹ thuật
 - Gián đoạn dữ liệu
 - Mất điện
 - Hỏng phần cứng
 - Những vấn đề về hạ tầng mạng

Phân loại gián đoạn

- Không phải thảm họa
- Thảm họa
- Đại thảm họa

Khôi phục dữ liệu

- Rút ngắn thời gian khôi phục dữ liệu
- Những lựa chọn sao lưu dữ liệu và phục hồi dữ liệu
- Ghi nhật ký dữ liệu (Data Journaling)

Lập kế hoạch khôi phục dữ liệu

Những chiến lược sao lưu và khôi phục dữ liệu

- Phân loại dữ liệu
- Quản lý dữ liệu dựa trên chính sách
- Ảo hóa lưu trữ
- Hợp nhất lưu trữ

Trung tâm dự phòng

- Phần mềm/Lưu trữ dữ liệu dự phòng
 - Vị trí
 - Tính bảo mật
 - Phương tiện vận chuyển
 - Những vấn đề môi trường
 - Tự xây dựng hoặc thuê
 - Tính sẵn sàng

Phân loại trung tâm dự phòng

- Hot Site
- Warm Site
- Cold Site

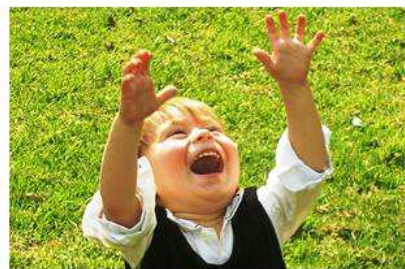
Những vấn đề liên quan đến trung tâm dự phòng

- Điều gì xảy ra nếu cùng lúc nhiều công ty cần đến trung tâm dự phòng
- Sự tương thích phần cứng
- Khả năng phục vụ
- Bảo mật
- Hậu cần

Những giai đoạn của một kế hoạch khôi phục sau thảm họa

- Khởi tạo dự án
- Thực hiện BIA
- Phát triển chiến lược và công nghệ
- Phát triển kế hoạch cho toàn doanh nghiệp
- Triển khai và kiểm tra kế hoạch
- Duy trì kế hoạch

Ưu tiên số một, trên tất cả là
Yếu tố CON NGƯỜI



Câu hỏi ?

Cám ơn !

SESSION 2: ĐÀO TẠO VÀ CHUẨN HÓA TRONG ATTT

Nội dung:

1. Đào tạo và chuẩn hóa ATTT
2. Định giá tài sản hệ thống thông tin
3. Đánh giá nguy cơ ATTT
4. Con đường trở thành chuyên viên an ninh mạng
5. Thảo luận

Người điều phối:



Ông Trịnh Ngọc Minh, Tiến sĩ Toán – Lý

- 15 năm kinh nghiệm quản trị mạng.
- 10 năm nghiên cứu và triển khai ATTT.
- Giảng viên Cisco Systems CCSI #31179, CCAI.
- Giảng viên Sun Microsystems (Solaris).
- Phó Giám đốc Khu Công nghệ Phần mềm – Đại học Quốc gia TpHCM kiêm Giám đốc Phòng thí nghiệm An ninh thông tin ISeLAB.

ĐÀO TẠO VÀ CHUẨN HÓA ATTT

(TS. Trịnh Ngọc Minh, ISeLAB, Khu CNPM ĐHQG-HCM)



Đào tạo và Chuẩn hóa An toàn Thông tin

Chủ trì: TRỊNH NGỌC MINH
Đại học Quốc gia TpHCM

Tiểu ban Đào tạo và chuẩn hóa An toàn thông tin

*Ngày hội An toàn thông tin phía Nam
Thành phố Hồ Chí Minh 18/11/2009*

Trịnh Ngọc Minh – Chủ trì tiểu ban

AN TOÀN THÔNG TIN

Lịch trình họp tiểu ban

Tổng quan bài toán bảo đảm an toàn thông tin theo chuẩn

Trịnh Ngọc Minh. Thời gian: 5'

Định giá tài sản hệ thống thông tin

Dương Ngọc Thái. Thời gian: 15' . Câu hỏi: 5'

Đánh giá nguy cơ an toàn thông tin

Đặng Hoàng Minh. Thời gian: 15' . Câu hỏi: 5'

Con đường trở thành chuyên viên an ninh mạng.

Sử Tam Nguyên. Thời gian 15'. Câu hỏi: 5'

Thảo luận.

Thời gian: 25 phút

Chú ý:

- Phiếu viết câu hỏi luôn sẵn sàng trong suốt thời gian diễn ra họp tiểu ban
- Nếu không có câu hỏi sẵn sàng sau trình bày, sẽ tiếp tục ngay trình bày sau . Câu hỏi có thể chuyển về thảo luận cuối giờ

AN TOÀN THÔNG TIN

Tổng quan bài toán bảo đảm an toàn thông tin theo chuẩn

Thành phố Hồ Chí Minh 18/11/2009

*TS Trịnh Ngọc Minh – ISeLAB, Khu CNPM ĐHQG-HCM
Giảng viên hệ thống Cisco (CCSI #31179) và Sun Microsystems*

tnminh@vnuhcm.edu.vn

AN TOÀN THÔNG TIN

Nội dung

- *An toàn thông tin – tương tự như bảo vệ tài sản thông thường*
- => Các nội dung chính của bài toán An toàn thông tin*

AN TOÀN THÔNG TIN

Bài toán bảo vệ tài sản

1. Xác định tài sản có giá trị, có thể bị người xấu “nhòm ngó”

- Tiền bạc, nữ trang
- Đồ đạc
- Đồ ăn thức uống

- Danh sách khách hàng
- Cơ sở dữ liệu thông tin thẻ tín dụng
- Thông tin tài khoản
- Thông tin hồ sơ dự thầu

=> Báo cáo về định giá giá trị tài sản số

AN TOÀN THÔNG TIN

Bài toán bảo vệ tài sản

2. Xác định nguy cơ bị mất tài sản

- Tiền bạc, nữ trang => nguy cơ lớn
 - Đồ đạc => nguy cơ trung bình
 - Đồ ăn thức uống => nguy cơ thấp nếu không có lũ lụt, nạn đói

 - Danh sách khách hàng => công ty đối thủ
 - Cơ sở dữ liệu thông tin thẻ tín dụng => hacker
 - Thông tin tài khoản => ???
 - Thông tin hồ sơ dự thầu => đối thủ cạnh tranh thầu
- => Báo cáo về đánh giá nguy cơ**

AN TOÀN THÔNG TIN

Bài toán bảo vệ tài sản

3. Triển khai công tác bảo vệ

A. Chi phí khắc phục sự cố > Đầu tư bảo vệ

=> đầu tư là hợp lý

B. Hacker kiếm được (vô hình và hữu hình) > Chi phí hacking

=> quyết định hack

Đầu tư bảo vệ tỷ lệ thuận với chi phí hacking

Tuân thủ ISO 27001/27002 là một phương án nên xem xét.

AN TOÀN THÔNG TIN



Định giá tài sản hệ thống thông tin

Dương Ngọc Thái,
CSO – Ngân hàng Đông Á

AN TOÀN THÔNG TIN

Đánh giá nguy cơ an toàn thông tin

Đặng Hoàng Minh, CISSP
Global CyberSoft (VN)

AN TOÀN THÔNG TIN

Con đường trở thành chuyên viên an ninh mạng

Th.S Sử Tam Nguyên,
Giảng viên hệ thống Cisco (CCSI)
Saigon CTT

AN TOÀN THÔNG TIN

Thảo luận

- Bài học kinh nghiệm, những cản trở khi đánh giá giá trị tài nguyên số đánh giá nguy cơ ATTT
- Xây dựng hệ thống ATTT theo chuẩn ISO 27xxx như thế nào ?
Bài học kinh nghiệm và khó khăn thuận lợi.
Lợi ích của việc theo chuẩn ISO 27xxx.
- Trung tâm cảnh báo sự cố máy tính :
một môi trường nghiên cứu và trưởng thành cho những ai yêu thích về an ninh thông tin.

.....

AN TOÀN THÔNG TIN



VNISA

VIETNAM INFORMATION SECURITY ASSOCIATION

www.vnisa.org.vn

HIỆP HỘI AN TOÀN THÔNG TIN VIỆT NAM
Phòng 11C1 – Tầng 11 – Tòa nhà CDC
25-27 Lê Đại Hành, Q. Hai Bà Trưng, Hà Nội
Tel/Fax: 844 – 6 278 6515

CHI HỘI VNISA PHÍA NAM
60 Nguyễn Văn Trỗi, Q. Phú Nhuận, TPHCM
Tel: 848 – 3 845 8518

Xin chân thành cảm ơn

ĐỊNH GIÁ TÀI SẢN HỆ THỐNG THÔNG TIN

(Ông Dương Ngọc Thái, CSO – Trưởng phòng ATTT, Ngân hàng Đông Á)



ĐỊNH GIÁ TÀI SẢN HỆ THỐNG THÔNG TIN

Người trình bày: *Dương Ngọc Thái*
CSO – Đông Á Bank



GIỚI THIỆU

DƯƠNG NGỌC THÁI

- Chief Information Security Officer – DongA Bank
- Blogger - <http://vnhacker.blogspot.com>
- Administrator – Hacker Vietnam Association - <http://www.hvaonline.net>
- Member – Team CLGT - <http://vnsecurity.net>
- Bug Hunter – Microsoft, Yahoo!, Sun, Apache Foundation, etc...

AN TOÀN THÔNG TIN



TỔNG QUAN

ĐỊNH GIÁ TÀI SẢN THÔNG TIN

- Tại sao cần phải định giá tài sản thông tin?
- Làm thế nào để định giá tài sản thông tin?
- Kết luận

AN TOÀN THÔNG TIN

TẠI SAO?

- Đầu tư hợp lý



AN TOÀN THÔNG TIN

TẠI SAO?

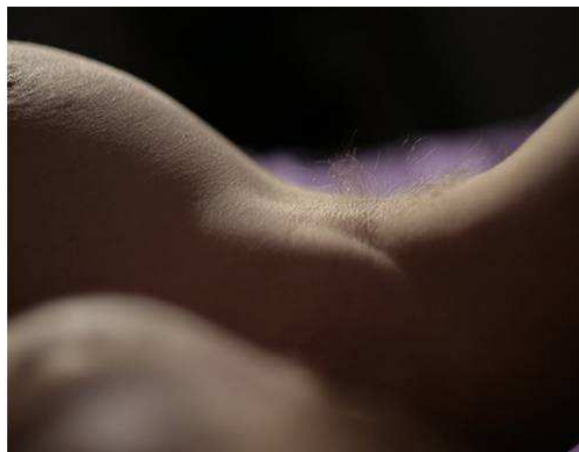
- Đầu tư hợp lý
- Quản lý rủi ro



AN TOÀN THÔNG TIN

NHƯ THẾ NÀO?

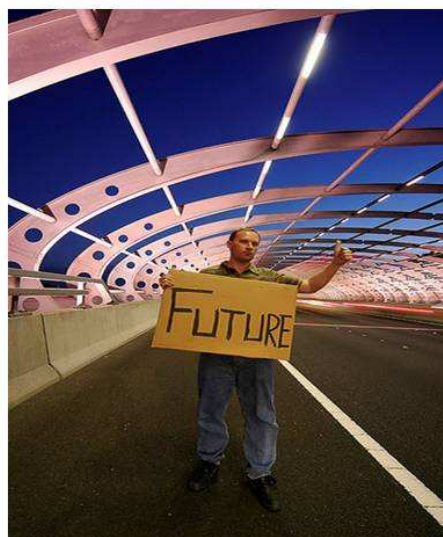
- Đúng ngữ cảnh



AN TOÀN THÔNG TIN

NHƯ THẾ NÀO?

- Đúng ngữ cảnh
- Hướng đến tương lai



AN TOÀN THÔNG TIN



NHƯ THẾ NÀO?

- Đúng ngữ cảnh
- Hướng đến tương lai
- Tạo giá trị kinh tế?

AN TOÀN THÔNG TIN



NHƯ THẾ NÀO?

- Đúng ngữ cảnh
- Hướng đến tương lai
- Tạo giá trị kinh tế?
 - Doanh thu



AN TOÀN THÔNG TIN

NHƯ THẾ NÀO?

- Đứng ngừ cảnh
- Hướng đến tương lai
- Tạo giá trị kinh tế?
 - Doanh thu
 - Lợi thế cạnh tranh
 - Bán giá cao hơn
 - Thu lợi nhiều hơn
 - Thị phần lớn hơn



AN TOÀN THÔNG TIN



VNISA

VIETNAM INFORMATION SECURITY ASSOCIATION

www.vnisa.org.vn

HIỆP HỘI AN TOÀN THÔNG TIN VIỆT NAM
Phòng 11C1 – Tầng 11 – Tòa nhà CDC
25-27 Lê Đại Hành, Q. Hai Bà Trưng, Hà Nội
Tel/Fax: 844 – 6 278 6515

CHI HỘI VNISA PHÍA NAM
60 Nguyễn Văn Trỗi, Q. Phú Nhuận, TPHCM
Tel: 848 – 3 845 8518

Xin chân thành cảm ơn

ĐÁNH GIÁ NGUY CƠ ATTT

(Ông Đặng Hoàng Minh, Senior IT Manager - GLOBAL CYBERSOFT (VN) JSC)

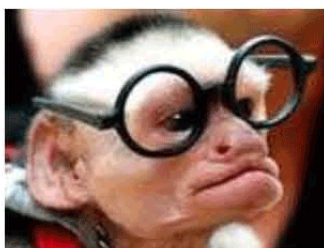


ĐÁNH GIÁ NGUY CƠ AN TOÀN THÔNG TIN

Người trình bày: ĐẶNG HOÀNG MINH, CISSP

Senior IT Manager
Global Cybersoft (VN) JSC
091 803 2431

- Bản Khoản của Cấp Lãnh Đạo Trong ATTT
- Mô Hình Quản Lý ATTT
- Quản Lý Rủi Ro Trong ISO 27001
- Quy Trình Quản Lý Rủi Ro
- Ví Dụ





Bản Khoản Của Lãnh Đạo Trong ATTT

- **Giám Đốc Điều Hành**
 - ✓ Làm thế nào đánh giá hiệu quả của giải pháp ATTT?
 - ✓ Tài sản nào cần bảo vệ? Tại sao?
 - ✓ Có mối đe dọa, điểm yếu nào?
 - ✓ Ảnh hưởng? Mức độ ảnh hưởng?
 - ✓ Làm thế nào loại trừ / giảm ảnh hưởng? Chi phí?
- **Giám Đốc Tài Chính**
 - ✓ Làm thế nào bảo đảm đầu tư cho ATTT hiệu quả?



AN TOÀN THÔNG TIN

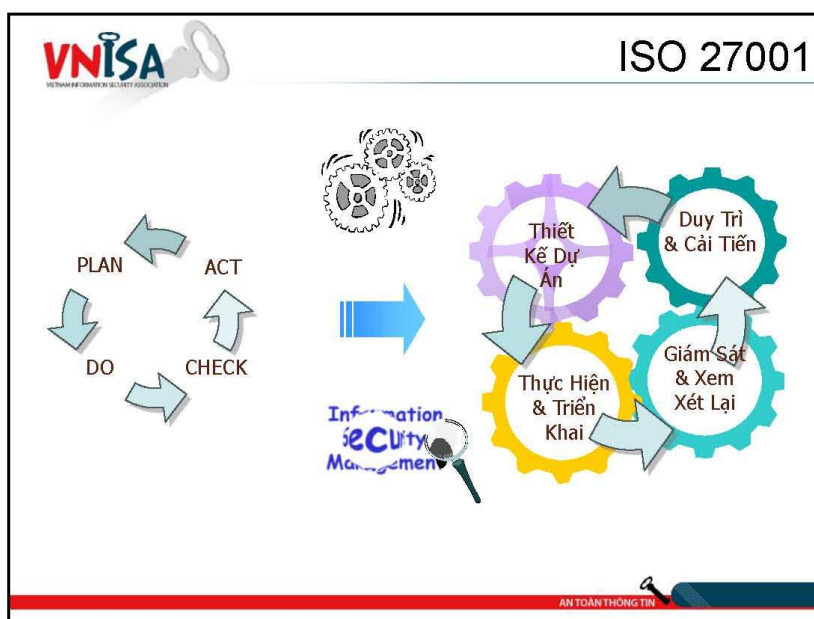
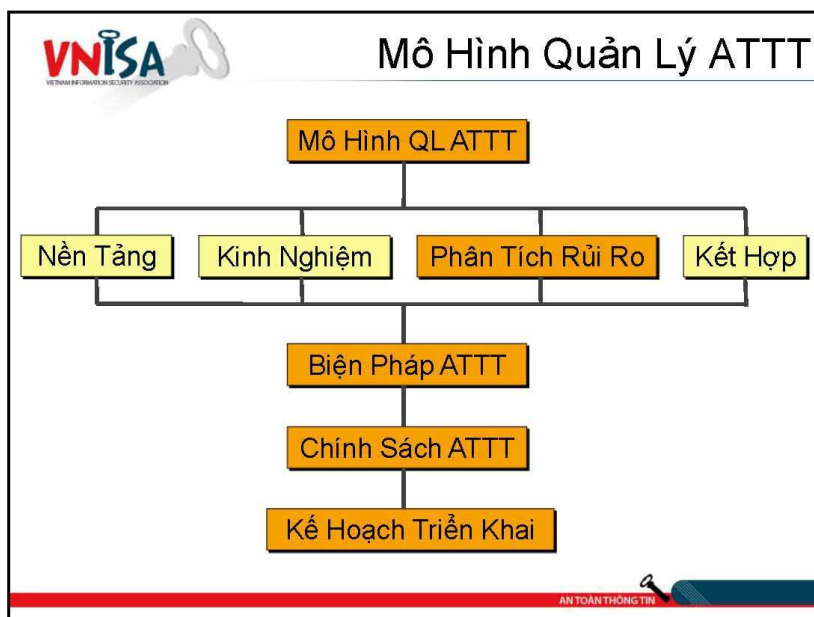


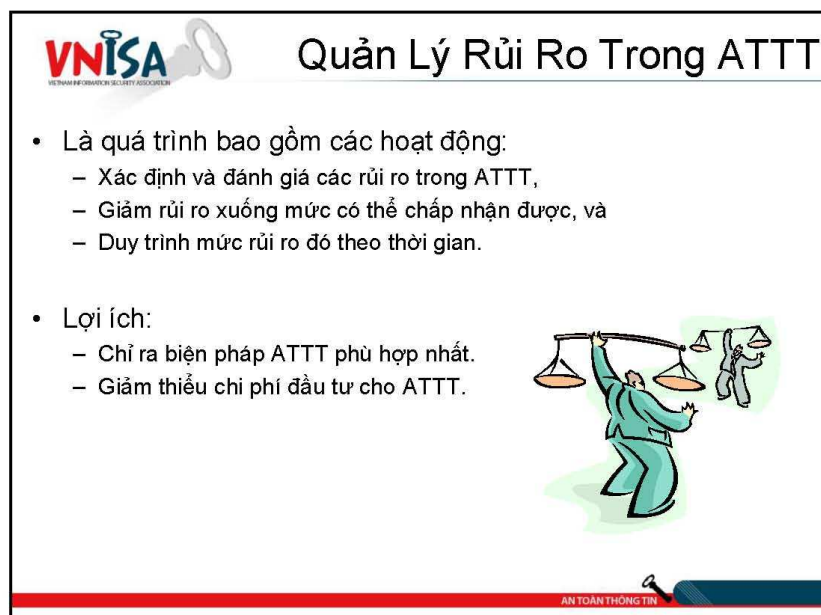
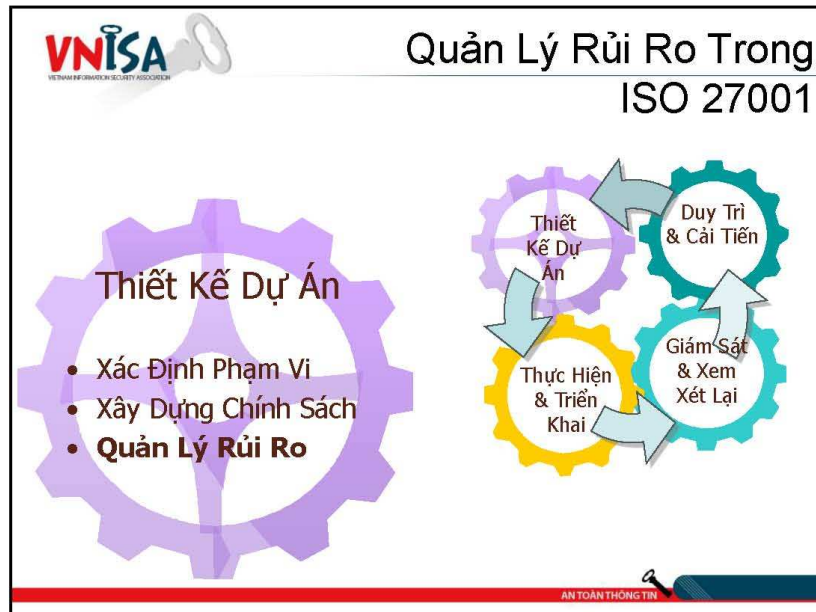
Bản Khoản Của Lãnh Đạo Trong ATTT

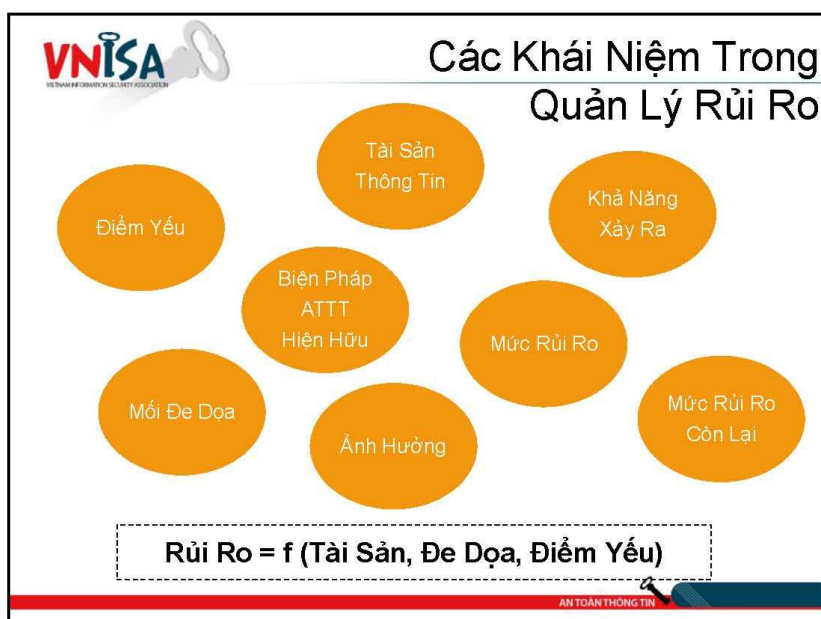
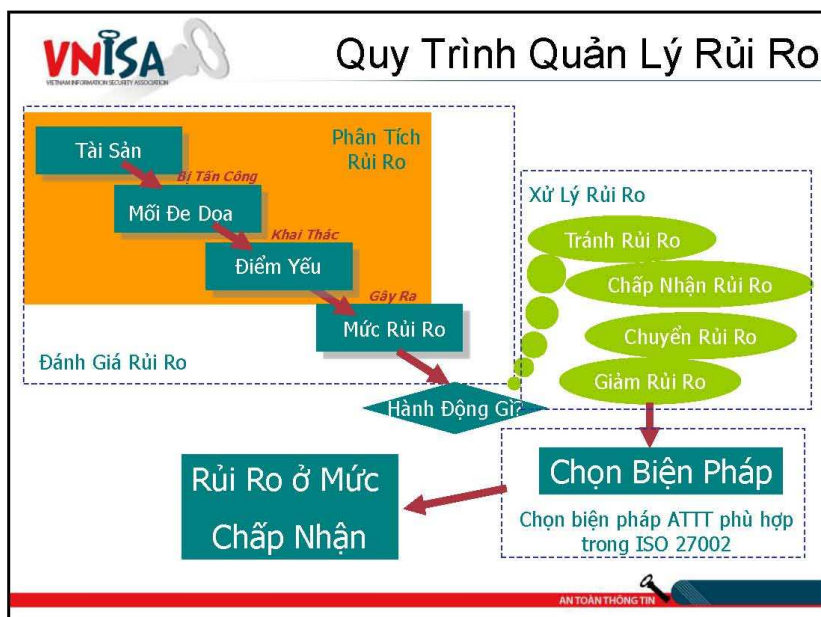
- **Giám Đốc IT, Giám Đốc ATTT**
 - ✓ Tài sản nào cần bảo vệ? Tại sao?
 - ✓ Có mối đe dọa, điểm yếu nào?
 - ✓ Ảnh hưởng? Mức độ ảnh hưởng?
 - ✓ Biện pháp ATTT nào phù hợp với tình hình công ty?
 - ✓ Làm thế nào duy trì & cải tiến mức độ ATTT theo thời gian?



AN TOÀN THÔNG TIN





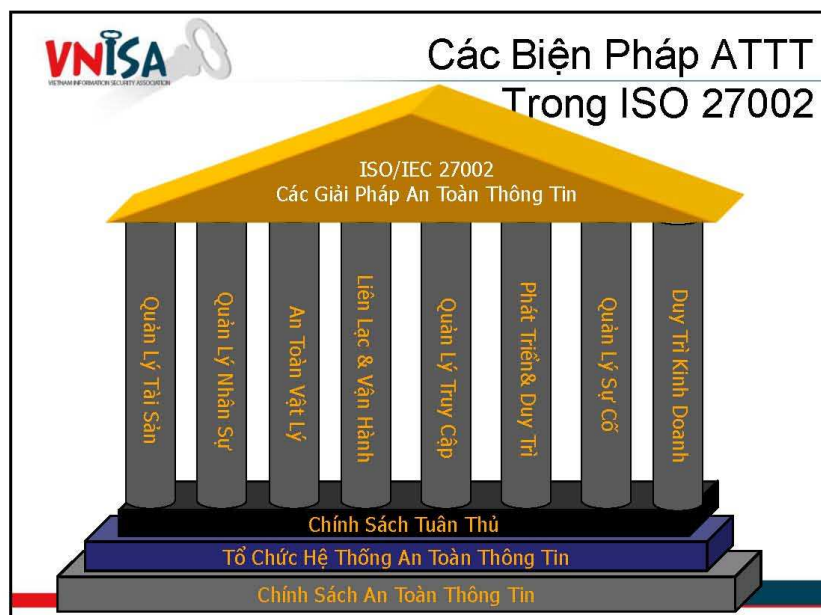




Ví Dụ

- Tài Sản: Tài khoản quản trị domain xyz.com ở NetworkSolutions
- Giá Trị Tài Sản: **Cao**
- Đe Dọa/Điểm Yếu: Bị chiếm quyền điều khiển/không có chính sách đổi mật khẩu thường xuyên, định kỳ
- Biện Pháp ATTT Hiện Hữu: Mật khẩu dài hơn 8 ký tự
- Khả Năng Xảy Ra: Trung Bình
- Ảnh Hưởng: **Cao**
- Mức Rủi Ro: **Cao**
- Tùy Chọn Xử Lý: Giảm Rủi Ro
- Biện Pháp Xử Lý: chính sách quản lý mật khẩu phải có yêu cầu thay đổi mật khẩu thường xuyên, định kỳ. (11.5.3)
- Mức Rủi Ro Còn Lại: **Thấp**

AN TOÀN THÔNG TIN





VNISA
VIETNAM INFORMATION SECURITY ASSOCIATION

www.vnisa.org.vn

Hiệp Hội An Toàn Thông Tin Việt Nam
Phòng 11C1 - Tầng 11 - Tòa nhà CDC
25-27 Lê Đại Hành, Q. Hai Bà Trưng, TP. Hà Nội
Tel/Fax: 844 - 6 278 6515

Chi hội VNISA Phía Nam
60 Nguyễn Văn Trỗi, Quận Phú Nhuận, TP. HCM
Tel: 848 - 3 845 8158 (ext: 1311)

Xin chân thành cảm ơn

Đặng Hoàng Minh, CISSP
Senior IT Manager
Global Cybersoft (VN) JSC.
091 803 2431

Đặng Hoàng Minh, CISSP

18/11/2009

7

CON ĐƯỜNG TRỞ THÀNH CHUYÊN VIÊN AN NINH MẠNG

(Th.s Sử Tâm Nguyên, Giảng viên hệ thống Cisco (CCSI) – SaigonCTT)



**Con đường trở thành chuyên viên
an ninh mạng**

ThS Sử Tâm Nguyên

Giảng viên Cisco (CCSI) – SaigonCTT

- Đảm bảo an toàn, an ninh và bảo mật cho hệ thống CNTT
- Cấp cao nhất là Chief Security Officer (CSO) - là người chịu trách nhiệm về an ninh của hệ thống thông tin và kinh doanh của doanh nghiệp.
- CSO thường điều hành về cả kỹ thuật và nhân sự để đảm bảo an ninh thông tin và an ninh trong kinh doanh

AN TOÀN THÔNG TIN

Yêu cầu kỹ thuật đối với một chuyên viên an ninh mạng – nền tảng (&&)

- Thành thạo về networking: Internet, TCP/IP, routing...
- Vững chắc về hệ điều hành: cơ chế quản lý và bảo vệ tiến trình, cơ chế phân quyền truy cập tài nguyên hệ thống...
- Hiểu rõ về lập trình, cơ sở dữ liệu, ứng dụng web...

AN TOÀN THÔNG TIN



Yêu cầu kỹ thuật đối với một chuyên viên an ninh mạng – chuyên ngành (||)

- Các cơ chế hoạt động các giao thức mạng liên quan tới an toàn thông tin
- Các điểm yếu của từng kiểu hệ điều hành
- Cách thức phát sinh các sơ hở trong lập trình cùng các ngôn ngữ lập trình khác nhau
- Các công nghệ mã hóa
- Chính sách an toàn thông tin

AN TOÀN THÔNG TIN



Yêu cầu kỹ thuật đối với một chuyên viên an ninh mạng – tư chất (&&)

- Nhạy cảm, tinh tế, sáng tạo trong công tác phát hiện xâm nhập, trong các cuộc “song đấu” với hacker.
- Kiên nhẫn, say mê nghề nghiệp,
- Ngăn nắp, tính kỷ luật cao, chu đáo, kỹ lưỡng
- Đạo đức nghề nghiệp, tránh được cám dỗ vật chất
- Chia sẻ, rộng mở với đồng nghiệp

AN TOÀN THÔNG TIN

Chuẩn bị gì cho nghề chuyên viên an ninh mạng?

AN TOÀN THÔNG TIN

Kiến thức nền tảng

- Tiếng Anh tối thiểu: đọc hiểu nhanh, chính xác.
- Kiến thức mạng Internet: CCNA là chứng chỉ nền tảng rất tốt của mạng tin học.
- Kiến thức hệ điều hành: Lý thuyết Hệ điều hành, MCSA/MCTS, căn bản về UNIX (Sun Solaris, LPI, HP-UX).
- Căn bản lập trình. Tốt nhất là C.

AN TOÀN THÔNG TIN

- Mạng: CCNP
- Máy chủ: MCSE, Sun Security Admin, HPUX admin hoặc Linux LPI admin.
- Chứng chỉ riêng của ATTT: CCSP, SCNP/ SCNA, MS Security, Security+, ISO 17799/27001/27002, CEH, foundstone...
- Đặc biệt: kiến thức về xâm nhập thử nghiệm (Penetration Testing).

- Certified Information Systems Security Professional (CISSP)
- Cisco Certified Internetwork Expert (CCIE) Security

- Nhiều con đường để đi đến đích: tự học, học theo cao đẳng/đại học, học theo chứng chỉ
- Theo học các trung tâm ủy quyền lấy chứng chỉ quốc tế cho phép trưởng thành trong nghề nghiệp một cách nhanh chóng và vững chắc.
- Có đam mê và quyết tâm, chắc chắn bạn sẽ thành công

Cám ơn đã lắng nghe

SESSION 3: ATTT TRONG THƯƠNG MẠI ĐIỆN TỬ

Nội dung:

1. Công nghệ xác thực hiện đại dựa trên Smartcard và kết hợp với Biometrics
2. Phòng tránh rủi ro cho máy chủ web với Microsoft System Center
3. Thảo luận + Bốc thăm trúng thưởng

Người điều phối:



Tiến sĩ Võ Văn Khang

Trưởng ban chứng thực số và thương mại điện tử VNISA, Phó Tổng Giám đốc NHTMCP Việt Á.

Ông Võ Văn Khang là chuyên gia về an toàn và bảo mật thông tin, đã tham gia tư vấn và xây dựng các giải pháp về ATTT cho nhiều đơn vị và doanh nghiệp. Ông cũng tham gia giảng dạy nhiều năm về ATTT tại ĐHQG TP.HCM

CÔNG NGHỆ XÁC THỰC HIỆN ĐẠI DỰA TRÊN SMARTCARD VÀ KẾT HỢP VỚI BIOMETRICS

(Ông Nguyễn Hữu Dũng, Tổng Giám Đốc Secude Vietnam)

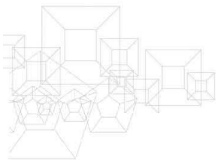


Công nghệ Xác thực Hiện đại Smart card - Biometrics

Trình bày: Nguyễn Hữu Dũng
SECUDE Vietnam

Nov 2009

- SECUDE: Tự giới thiệu
- Công nghệ thẻ thông minh
 - Định nghĩa, đặc điểm và lợi ích của công nghệ
 - Phương pháp xác thực hiện đại dựa trên thẻ thông minh
 - Kết hợp với sinh trắc học (Biometrics)
- Các phần mềm ứng dụng dựa trên công nghệ thẻ thông minh
 - Token lifecycle management system
 - Single Sign On in SAP and Non-SAP environment
 - Các sản phẩm khác
- Hỏi và đáp



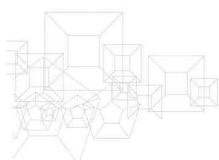
SECUDE AG

- SECUDE AG được thành lập vào năm 1996 bắt đầu từ sự hợp tác giữa SAP AG và Fraunhofer Institute in Germany
- Là một trong những công ty hàng đầu cung cấp các sản phẩm và giải pháp toàn diện an toàn bảo mật thông tin cho môi trường SAP cũng như cho môi trường thông tin doanh nghiệp nói chung
- Trụ sở chính ở Thụy Sĩ (Switzerland)

SECUDE Vietnam

- Thành lập 02-2007
- Một trong những trung tâm giải pháp, công nghệ và marketing của SECUDE AG



SECUDE GLOBAL FOOTPRINT


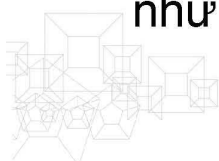
- Bringing the SWISS standard of excellence and innovation into the global IT Security market

4

11/9/2009

© 2009 SECUDE AG

- Định nghĩa
 - Là thiết bị di động được tích hợp một microcomputer chip và một vùng nhớ (memory) để lưu trữ dữ liệu
 - Data được trao đổi thông qua một đầu đọc (smart card reader), có 2 loại contact và contactless
 - Theo tiêu chuẩn ISO/IEC 7816 (contact) và ISO/IEC 14443 (contactless)
 - Có loại được tích hợp reader-card vào một thiết bị như USB based token



5

11/9/2009

© 2009 SECUDE AG

- Theo tiêu chuẩn ít nhất trên 10.000 lần đọc/ghi
- Dung lượng có thể lên đến 128k
- Thẻ thông minh tiêu chuẩn phải qua kiểm định với các yếu tố ngoại vi như độ ẩm, x-ray, v.v... đảm bảo độ bền
- Rất khó hoặc không thể làm giả smart card (duplicate) và sao chép dữ liệu của nó so với các loại card khác (thẻ từ)
- Thiết bị lưu trữ cá nhân di động tiện dụng



- Thiết bị có đặc tính bảo mật và an toàn cao
 - Tự xác thực (Authenticate) người sử dụng với PIN (Personal Identification Number)
 - Khả năng xác thực 2 yếu tố (sở hữu và PIN)
 - Các chức năng mã hóa sẵn có trên card giúp bảo mật dữ liệu lưu trong card
 - Vùng lưu trữ PIN là không thể xâm phạm
 - Một số đầu đọc (reader) trang bị PIN pad để nhập PIN tránh được nguy cơ Keylogger khi nhập từ bàn phím máy tính
 - Kết hợp với sinh trắc học (Biometric) tạo thành một cơ chế xác thực 3 yếu tố

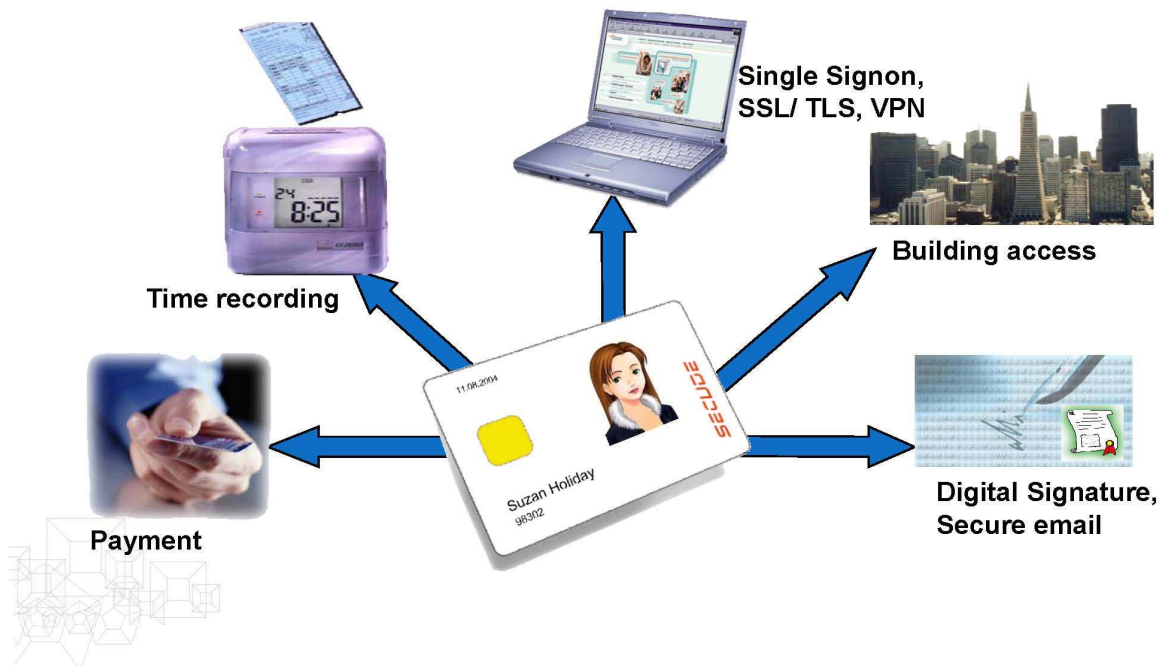


+

PIN

SECUDE

Nhiều chức năng sử dụng



8

11/9/2009

© 2009 SECUDE AG

SECUDE

Các chức năng sẵn có

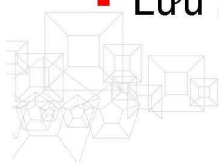
- Các chức năng sẵn có (on-card functions)
 - Hệ điều hành (COS – Chip Operating System) được tích hợp vào chip của card
 - Bảo vệ thẻ thông minh với những trường hợp có tính xâm nhập dữ liệu bên trong thẻ (lock card)
 - Sản sinh ra các khóa mật mã khác nhau (đồng bộ và không đồng bộ), chữ ký số phục vụ cho mục đích bảo mật dữ liệu của người dùng
 - Thực thi các tác vụ xác thực, mã hóa/giải mã cũng như thực thi tác vụ chữ ký điện tử (digital signature)
 - Các khóa bí mật (Private key/secret key) được sản sinh không thể bị sao chép ra khỏi thẻ

9

11/9/2009

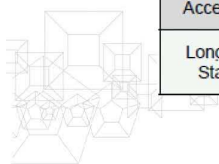
© 2009 SECUDE AG

- Thẻ thông minh kết hợp với PIN được sử dụng để thực thi các phương pháp xác thực hiện đại
 - Lưu trữ password của người sử dụng để đăng nhập vào các ứng dụng khác nhau
 - Sản sinh và lưu trữ chứng chỉ số (digital certificate) của người dùng để xác thực danh tính người dùng trong môi trường nền tảng khóa công cộng (PKI)
 - Lưu trữ các mẫu sinh trắc học (Biometric template) để xác thực danh tính
 - Lưu trữ các khóa đồng bộ để mã hóa và giải mã
 - Lưu trữ các mẫu của OTP - One Time Password



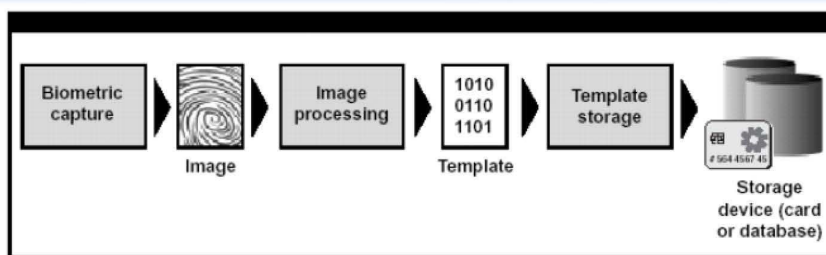
- Tiến trình xác thực định danh dựa vào các tính chất và đặc điểm sinh trắc của con người
- Tùy theo tính chất hệ thống mà xác định phương pháp phù hợp
- Đang ngày càng phổ biến trong các hệ thống định danh hiện đại
- Đang ngày càng được chuẩn hóa (<http://www.biometrics.org/>)

Characteristic	Fingerprints	Hand Geometry	Retina	Iris	Face	Signature	Voice
Ease of Use	High	High	Low	Medium	Medium	High	High
Error Incidence	Dryness, dirt, age	Hand injury, age	Glasses	Lighting	Lighting, age, glasses, hair	Changing signatures	Noise, colds
Accuracy	High	High	Very high	Very high	High	High	High
User Acceptance	Medium	Medium	Medium	Medium	Medium	High	High
Long-Term Stability	High	Medium	High	High	Medium	Medium	Medium

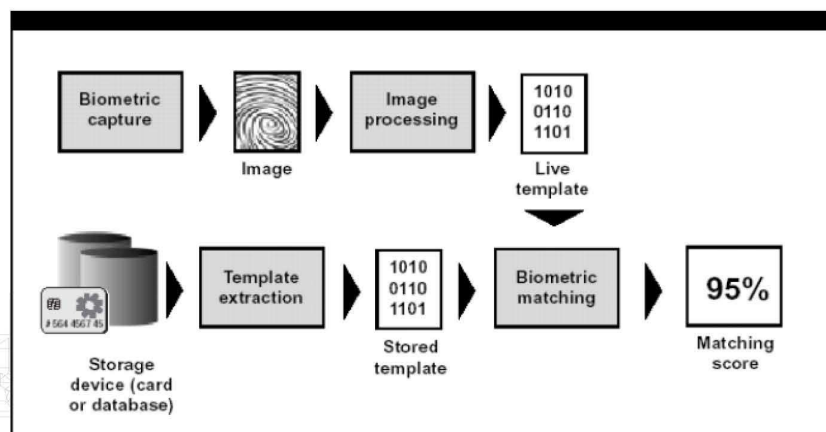


SECUDE

Xác thực dựa trên sinh trắc



Tiến trình đăng ký người sử dụng



Tiến trình xác thực người sử dụng

12

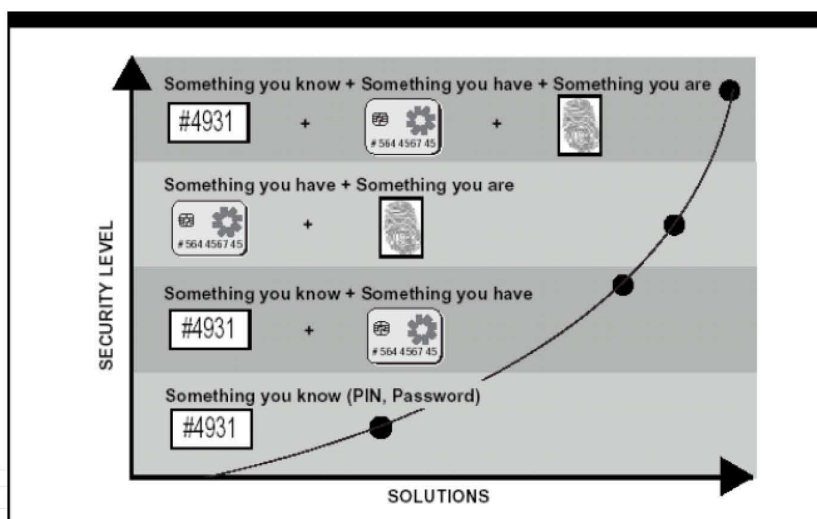
11/9/2009

© 2009 SECUDE AG

SECUDE

Thẻ thông minh – Sinh trắc

- Xác thực dựa trên sinh trắc của con người là một phần của một hệ thống xác thực hiện đại dựa trên 3 yếu tố



13

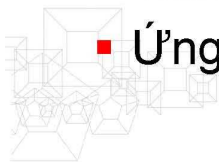
11/9/2009

© 2009 SECUDE AG

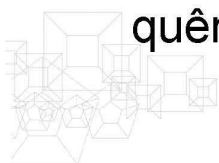
- Mẫu sinh trắc của người dùng có thể được lưu vào thẻ thông minh nhằm làm tăng khả năng xác thực người dùng
 - Tiến trình kiểm tra xác thực có thể được thực hiện ngay trên thẻ không cần cơ sở dữ liệu (database), cải thiện hiệu năng hệ thống
 - Tăng khả năng xác thực định danh người dùng
 - Tăng tính bảo mật riêng tư, người sử dụng thẻ có thể quản lý thông tin riêng tư trong thẻ
 - Hỗ trợ nhiều phương thức xác thực định danh khác nhau tùy theo nhu cầu

- Thẻ thông minh đem lại lợi ích to lớn nhưng cần được sử dụng một cách đúng đắn
 - Luôn rút thẻ ra khỏi thiết bị đọc (reader) một khi không sử dụng và giữ thẻ cẩn thận bên mình
 - Luôn dùng số PIN khó đoán
 - Mất thẻ phải báo ngay cho người quản lý hệ thống thẻ
 - Không cho mượn thẻ
- Bảo quản tốt thẻ thông minh
- Luôn coi trọng và tuân thủ các quy trình bảo mật được thiết lập Thẻ thông minh và xác thực sinh trắc chỉ là một trong các công cụ trong một quy trình xác thực hiện đại và hiệu quả

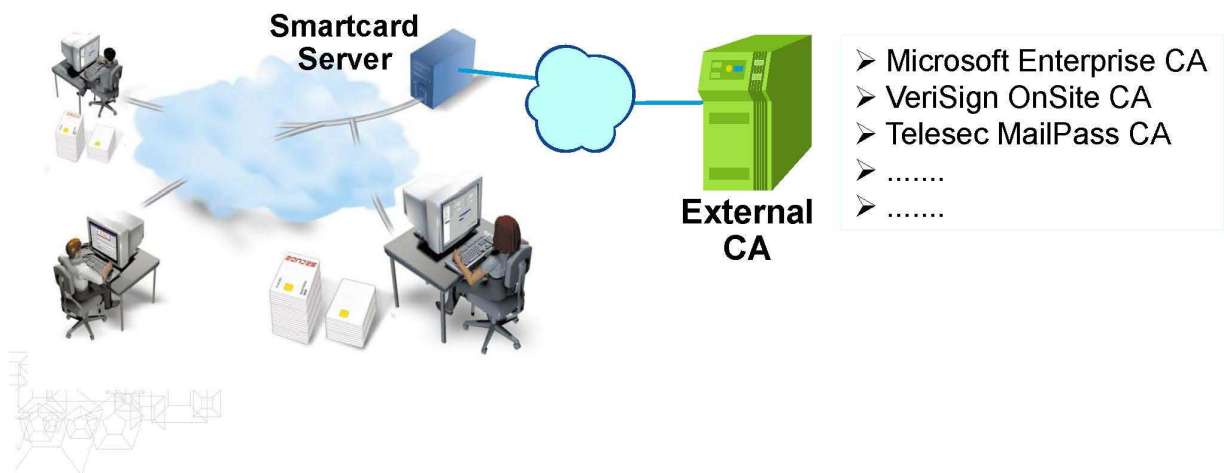
- Thẻ thông minh có thể được sử dụng trong nhiều lĩnh vực khác nhau, đặc biệt trong các tổ chức đòi hỏi bảo mật cao như chính phủ, ngân hàng .vv...
- Các ứng dụng thường thấy
 - Hệ thống cấp phát và quản lý thẻ thông minh (Smart card management system)
 - Hệ thống quản lý định danh (Identity Management)
 - Ứng dụng Single Sign-on



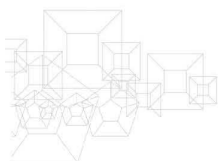
- Hệ thống cấp phát và quản lý thẻ thông minh (Smart card management system)
 - Quản lý vòng đời của một thẻ thông minh từ lúc cấp phát (issue) cho đến khi thu hồi (withdraw)
 - Cấp phát chứng chỉ số và các khóa liên quan cho người dùng
 - Hỗ trợ người sử dụng trong việc quản lý PIN (reset PIN)
 - Hỗ trợ người dùng trong việc quản lý thẻ (mất thẻ, quên thẻ)

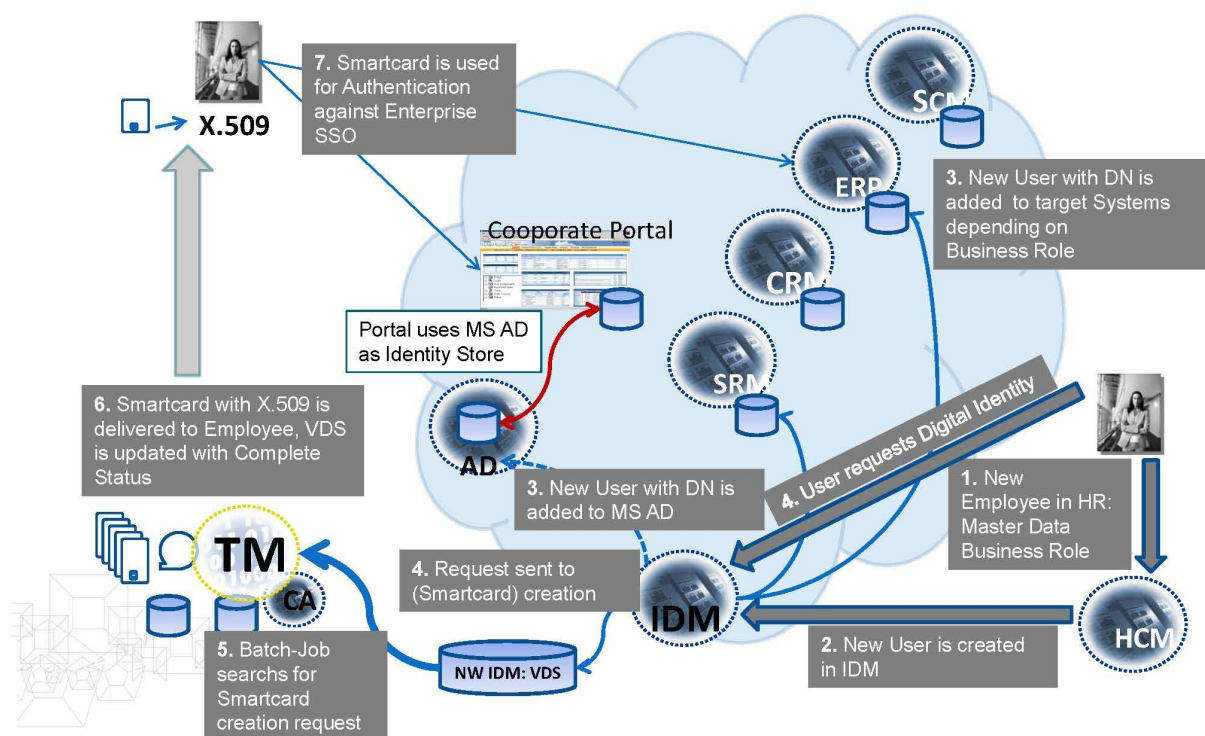


- Dễ dàng liên kết và tích hợp với một hệ thống CA để quản lý chứng chỉ số (certificate)
- Có thể được tích hợp một hệ thống quản lý danh tính (Identity Management)



- Hệ thống quản lý danh tính, xác thực và phân bổ quyền đăng nhập và sử dụng hệ thống cho các cá nhân trong một tổ chức
- Thẻ thông minh được cấp phát và sử dụng trong tổ chức để xác thực định danh người sử dụng





20

11/9/2009

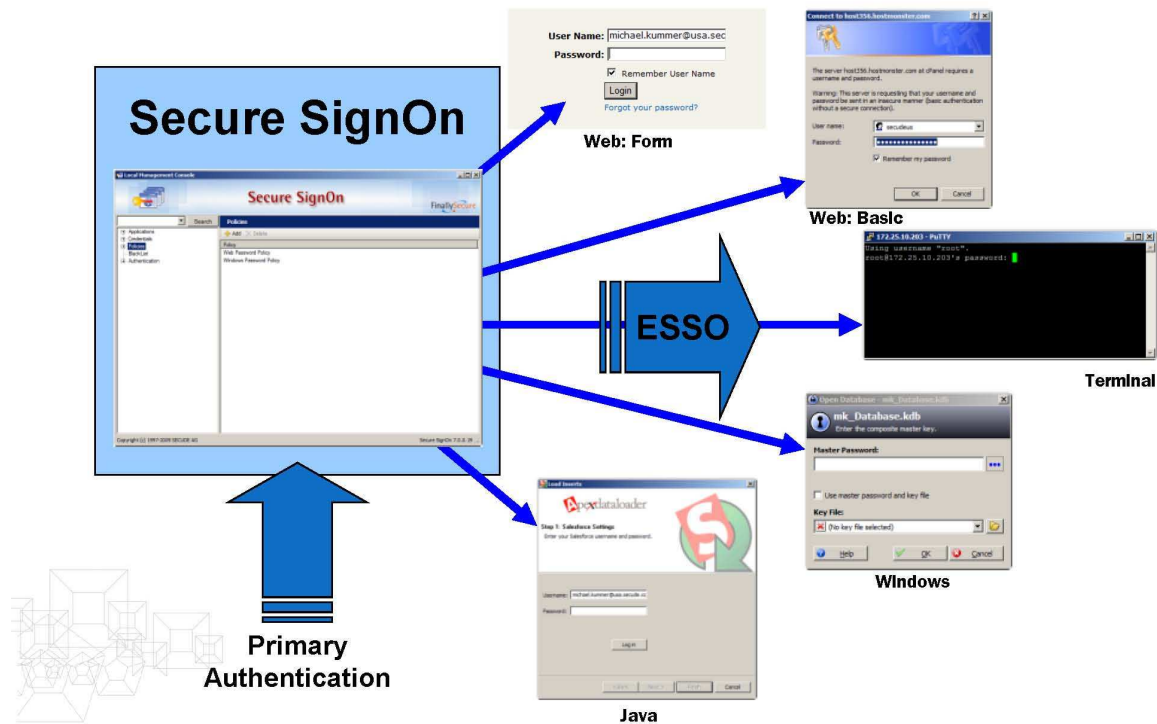
© 2009 SECUDE AG

- Thông tin của tài khoản người dùng (tên, password) sẽ được lưu vào thẻ thông minh và mã hóa
- Hỗ trợ đăng nhập windows bằng chứng chỉ số (certificate login)
- Hỗ trợ đăng ký tài khoản mới và ứng dụng tương ứng
- Tự động điền thông tin tài khoản vào form đăng nhập, người dùng không cần phải gõ vào
- Hỗ trợ sản sinh ra password tự động theo một luật lệ được người dùng định nghĩa (password policy)
- Cho phép người dùng quản lý tài khoản và các ứng dụng đăng nhập tương đương

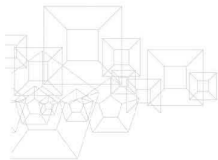
21

11/9/2009

© 2009 SECUDE AG



Xin chân thành cảm ơn.



Tóm tắt sơ lược về Ông Nguyễn Hữu Dũng:



Với hơn 10 năm kinh nghiệm trong ngành công nghệ phần mềm máy tính, Ông Nguyễn Hữu Dũng đang là Tổng Giám Đốc, chịu trách nhiệm chính về mảng giải pháp và công nghệ cho tập đoàn ở Việt Nam. Cùng với các trung tâm giải pháp khác của tập đoàn ở nhiều nơi trên thế giới, SECUDE Việt Nam đang từng bước góp phần vào việc nâng cao chất lượng và thương hiệu của SECUDE trên thị trường thế giới.

Trước khi gia nhập SECUDE vào đầu năm 2007, ông Nguyễn Hữu Dũng từng đảm nhận các vị trí quản lý kỹ thuật quan trọng trong các công ty gia công phần mềm nước ngoài ở Việt Nam như SDC (Saigon Software Development Company) hay AdnovaTech Solution Corp...

PHÒNG TRÁNH RỦI RO CHO MÁY CHỦ WEB VỚI MICROSOFT SYSTEM CENTER

*(Ông Vũ Nguyễn Cao Sơn, Chuyên gia công nghệ cho mảng tài chính
và tổng công ty của Microsoft phía Nam)*

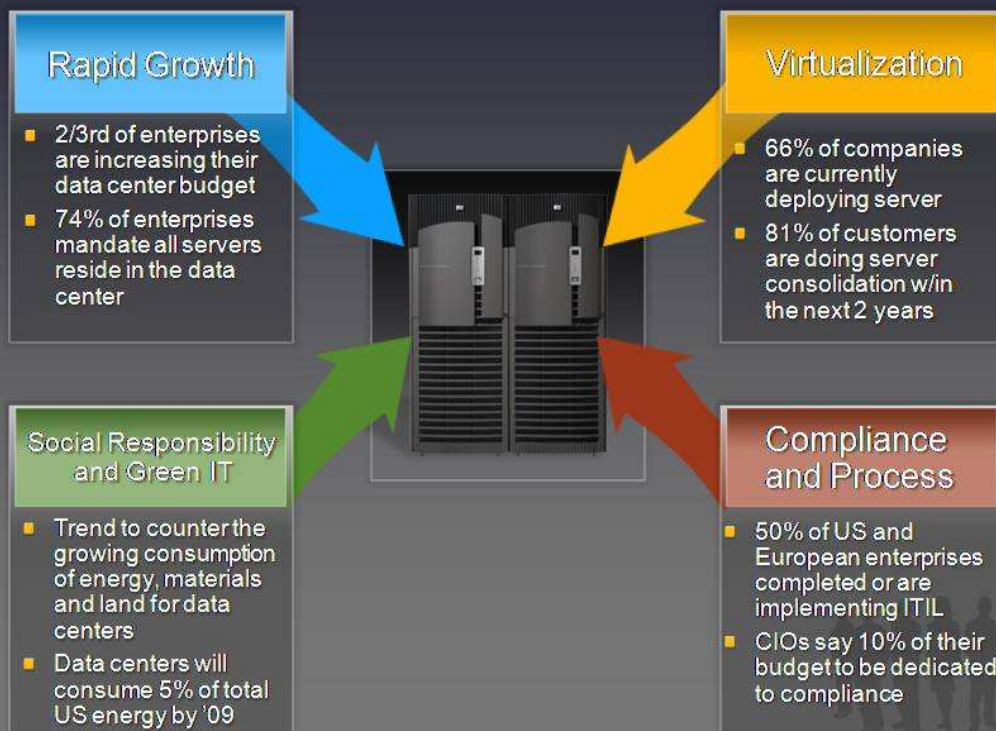


Agenda

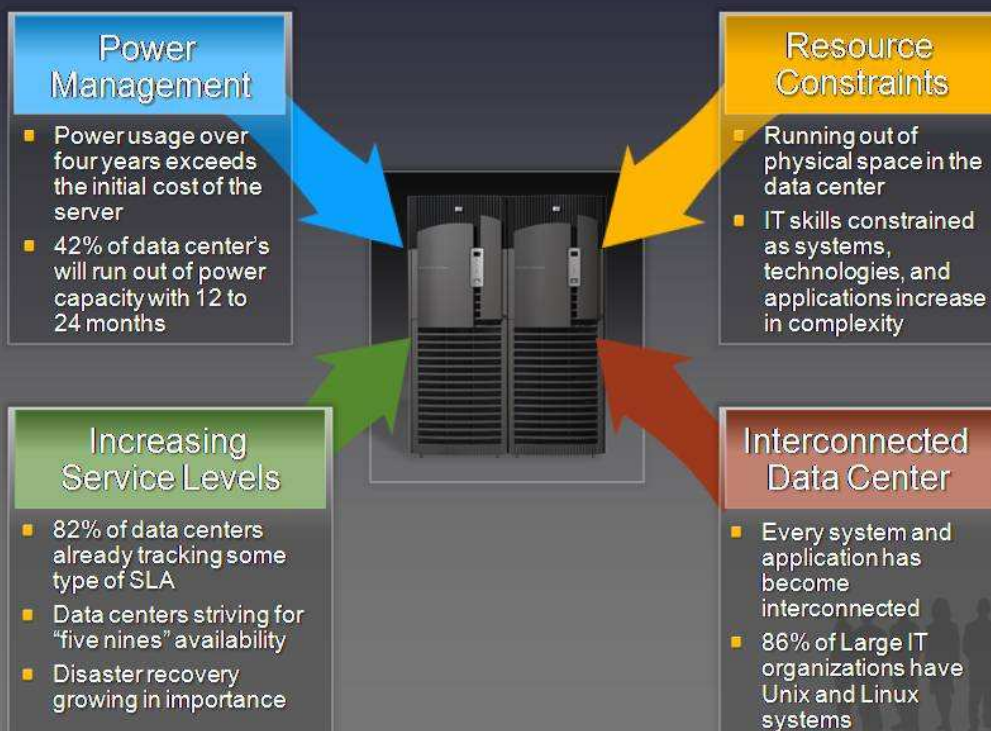
- The Changing Data Center
- Microsoft's Approach
- Solutions for Web Infrastructure
- Some Demo....



Changes Affecting the Data Center



Data Center Pressures



Adapting to Market: Datacenter Evolution

Traditional Datacenter Virtualized Datacenter Private Cloud Public Cloud

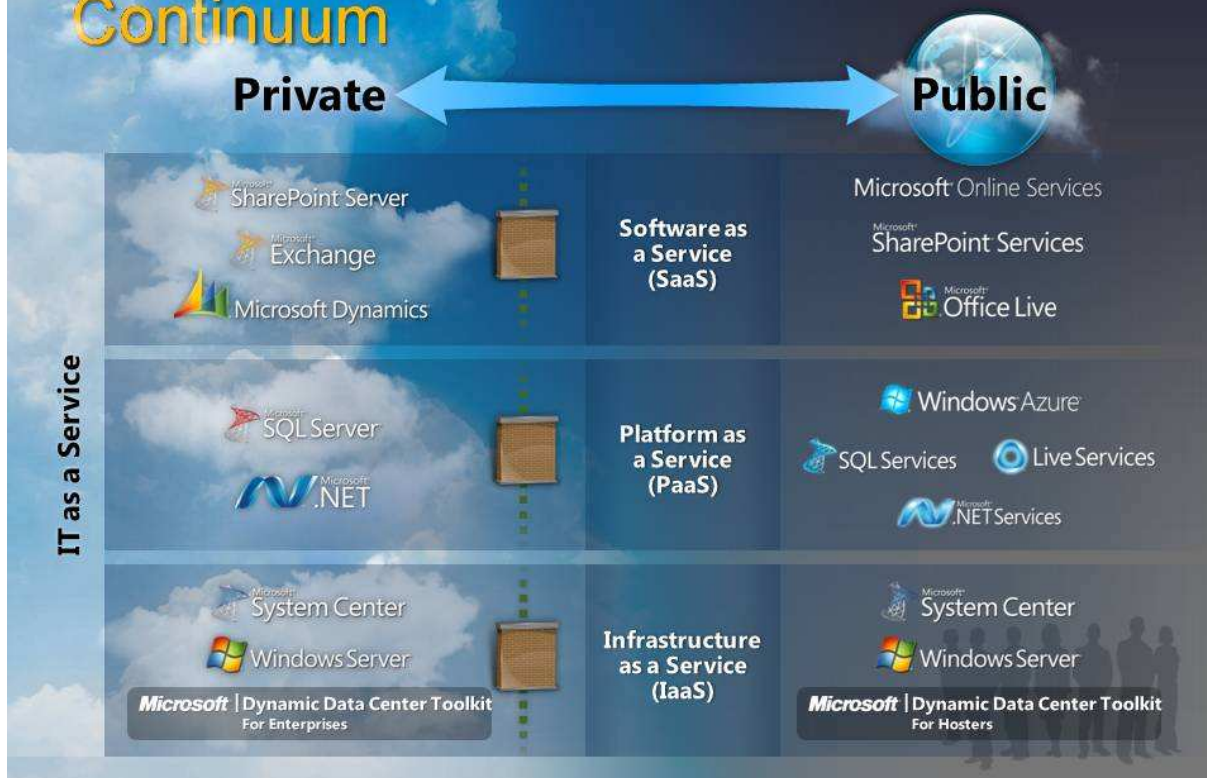


Agenda

- The Changing Data Center
- **Microsoft's Approach**
- Solutions for Web Infrastructure
- Some Demo....



Microsoft Cloud Computing Continuum



Management Moves Front and Center

Servers must be configured and optimized

- Increasing power and space concerns
- Greater number of deployments and updates



Must be available and responsive

- Higher service levels demanded
- Importance of interoperability and openness



Must support compliance, process and controls

- More internal and external pressures
- Access drives security and protection



Must ensure business continuity and dependable recovery

- Centralized assets drives disaster contingency
- Virtualization for business continuity



Agenda

- The Changing Data Center
- Microsoft's Approach
- **Solutions for Web Infrastructure**
- Some Demo....



Managing Server Compliance

Controls Must Be Enforced Across Complete Data Center

- Greater flexibility but lower control with server virtualization
- Centralization of services into data center increases need for centralized compliance



Security Event Collection Must Be Cost Effective

- Volume of data that must be collected increasing dramatically
- More external and internal demand for security event reports



Security and Server Management Must Reduce Risk

- Data and application access risks drive need to look across security disciplines
- Compliance requirements require holistic security approach



System Center Server Compliance Solution Supports Enhanced Compliance

Configuration Controls and Reporting



- Desired server configuration management
- Asset intelligence reporting
- Security vulnerability assessment

Centralized Security Auditing



- Collection and consolidation of security events
- Reporting to meet audit requirements
- Default and custom reporting



Server Compliance Management

Knowledge Driven Server Compliance Management

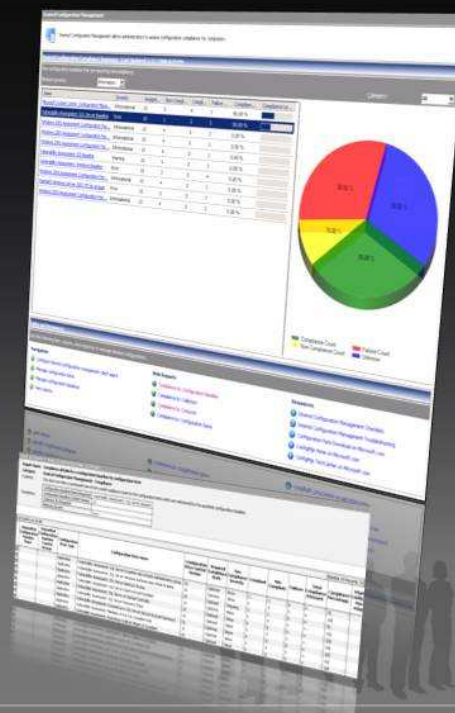
Develop, then automatically deploy and manage configuration baselines

- OS, application and user settings
- Update and patch installation
- Security settings

Dashboards provide IT management with holistic view of configuration compliance

- Detail reports support targeted action

Automate configuration remediation for all required servers



Server Compliance Management

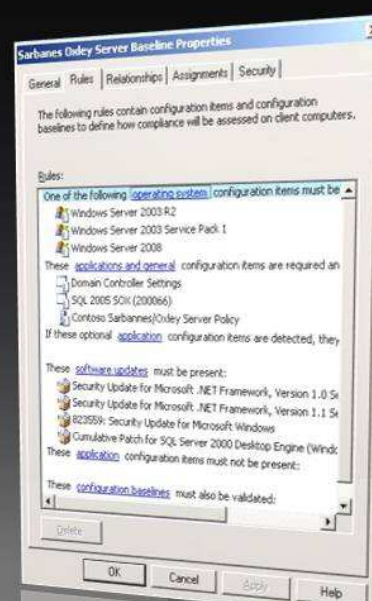
Built In Server Compliance Best Practices

Configuration Packs support compliance through Desired Configuration Management:

- Configuration items, settings and values
- Targeted assessment of servers against specific configuration baselines
- Customizable settings

Specific Configuration Packs for:

- Sarbanes-Oxley
- Federal Information Security Management Act (FISMA)
- Gramm-Leach-Bliley (GLBA)
- Health Insurance Portability and Accountability Act (HIPAA)
- European Union Data Protection Directive (EUDPD)



Server Compliance Management

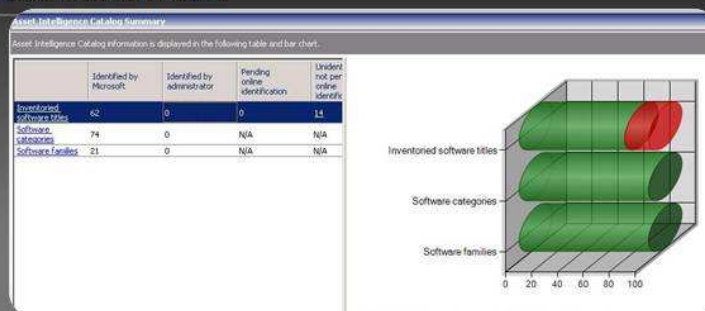
Asset Intelligence Reporting

Reducing license compliance risk through reporting

- Hardware and software inventory
- Software license usage information

Software catalogue based asset reporting

- Regularly refreshed central via Microsoft service
- Online, automated synchronization
- Ability to add custom data



Server Compliance Management

Security Vulnerability Assessment

Security compliance reporting

- Security specific Configuration Packs
- Best practices for planning, setting, monitoring and remediating security baselines

Reduced effort to manage risk in the data center

- Automate security assessments
- Support change management for security settings



Centralized Auditing of Security Events

Meet Security Audit Reporting Needs

Collection and consolidation of server security log information

- Near real-time consolidated security log information from across data center
- Extensive reporting for external and internal compliance requirements

Custom and default reporting includes:

- Account management
- Access violation
- Policy changes
- System integrity

Microsoft System Center Operations Manager 2007

Password Change Attempts by Non-owner

EventID 4740 indicates password change attempt and success. It includes a password result. The report displays any password or password attempts for non-owner users from the account table.

Date/Time	Computer	Source	User Account	Changed By
4/2/2008 12:34 AM	CONF000002	CONF000	MEMBER1	Administrator
4/2/2008 12:34 AM	CONF000002	CONF000	MEMBER2	Administrator
4/2/2008 12:34 AM	CONF000002	CONF000	MEMBER3	Administrator
4/2/2008 12:34 AM	CONF000002	CONF000	MEMBER4	Administrator
4/2/2008 12:34 AM	CONF000002	CONF000	MEMBER5	Administrator
4/2/2008 12:34 AM	CONF000002	CONF000	MEMBER6	Administrator
4/2/2008 12:34 AM	CONF000002	CONF000	MEMBER7	Administrator
4/2/2008 12:34 AM	CONF000002	CONF000	MEMBER8	Administrator
4/2/2008 12:34 AM	CONF000002	CONF000	MEMBER9	Administrator
4/2/2008 12:34 AM	CONF000002	CONF000	MEMBER10	Administrator

End to End Monitoring

Proactive platform, application and service-level monitoring

Challenges Addressed

- Unintended configuration changes resulting in greater cost and risk
- Heterogeneous mix of services, applications and servers causing inability to find root cause and increased downtime
- Increasing service level agreements difficult to meet

End to End Monitoring Capabilities

- Availability, performance, and configuration monitoring to proactively address IT issues
- Deep application and service -level monitoring



"I can provide our system administrators with more in-depth monitoring and more explicit alerting. We can configure server reports to show downtime warnings, downtime events, and the start time and end time of every occurrence. We can also quickly learn why a server experienced downtime—whether it was a power outage, a hardware or software malfunction, or a server maintenance issue."

- Paul Johnson, Windows Monitoring Architect & Systems Engineer, Gates Corp.

End to End Monitoring

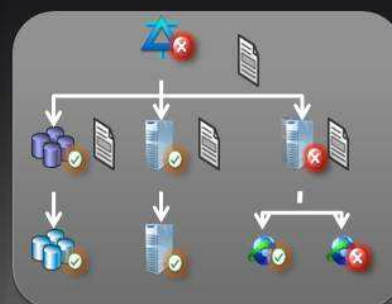
Proactive platform, application and service-level monitoring

Availability, performance, and configuration monitoring to proactively address IT issues

- Monitor multiple platforms (e.g. Windows, Linux, and UNIX) for both your physical and virtual servers
- Proactively keep systems up and running with best-practice knowledge on how to resolve problems
- Allow configuration change monitoring by identifying configuration errors and changes
- Diagram data center operations and visualize status
- Report on status of configuration and system issues affecting availability, performance, and reliability

Deep application and service-level monitoring

- Monitor service levels across applications and IT processes through operational IT service views
- Track and report service levels through dashboards
- Extend to monitor non-Microsoft applications with partners
- Guidance and best practice services to meet service-level goals and improve IT productivity



Data Protection and Recovery

Backup and restore & business continuity through virtualization

Challenges Addressed

- Demand for business continuity driving increased costs related to geocustering and new technology investments
- Centralized data centers causing more risk of downtime and data loss in the event of a disaster or outage

Data Protection and Recovery Capabilities

- Ensure business continuity and responsiveness with server virtualization management
- Recover and restore physical and virtual environments after an outage, data loss or corruption

AutoNation

"We really liked the looks of [System Center] for three key reasons, its disk-to-disk-to-tape design, the fact that we could eliminate full backups altogether and simply take snapshots, and its disaster recovery features."

- Ed Olson, Lead Windows Infrastructure Engineer, AutoNation



Data Protection and Recovery

Backup and restore & business continuity through virtualization

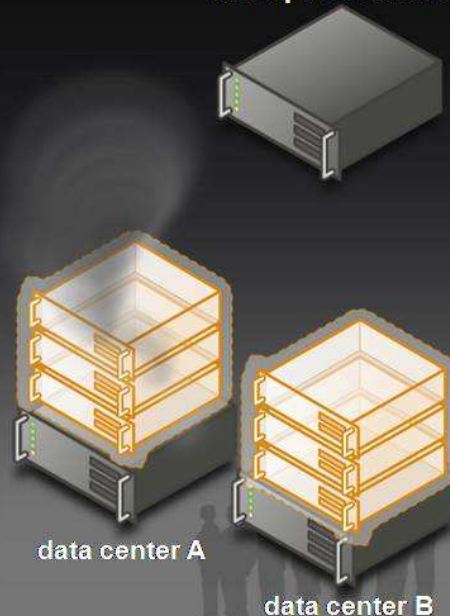
Ensure business continuity and responsiveness with server virtualization management

- Distribute workloads over locations to ensure continuous and uninterrupted business operations
- Provide replication and movement of virtual machines and applications for planned backups

Recover and restore physical and virtual environments after an outage, data loss or corruption

- Allows backup and recover of mission critical workloads
- Perform continuous data protection using integrated disk and tape media
- Enable rapid and reliable recovery from disk as well as long term data protection through tape based backup
- Recover both physical and virtual systems after an outage, data loss or corruption
- Allows geoclustering for disaster recovery and business continuance by physically separating cluster nodes

backup and restore



Managing the Server Lifecycle

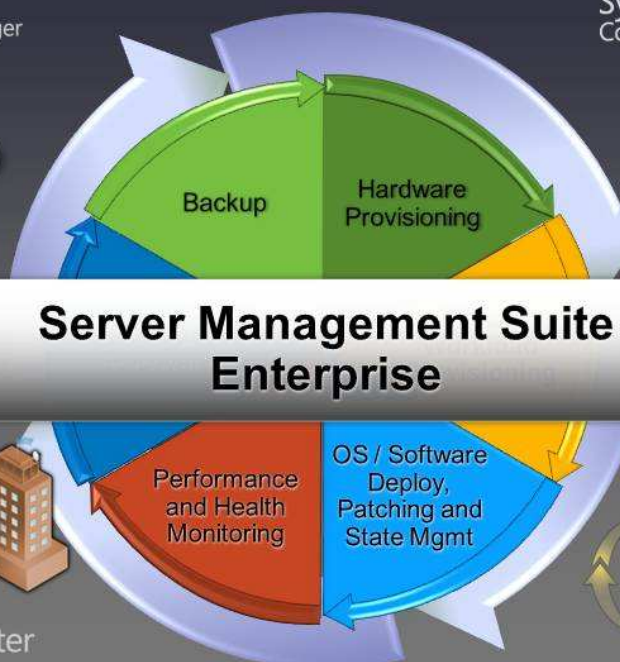
Microsoft®
System Center
Data Protection Manager



Microsoft®
System Center
Configuration Manager



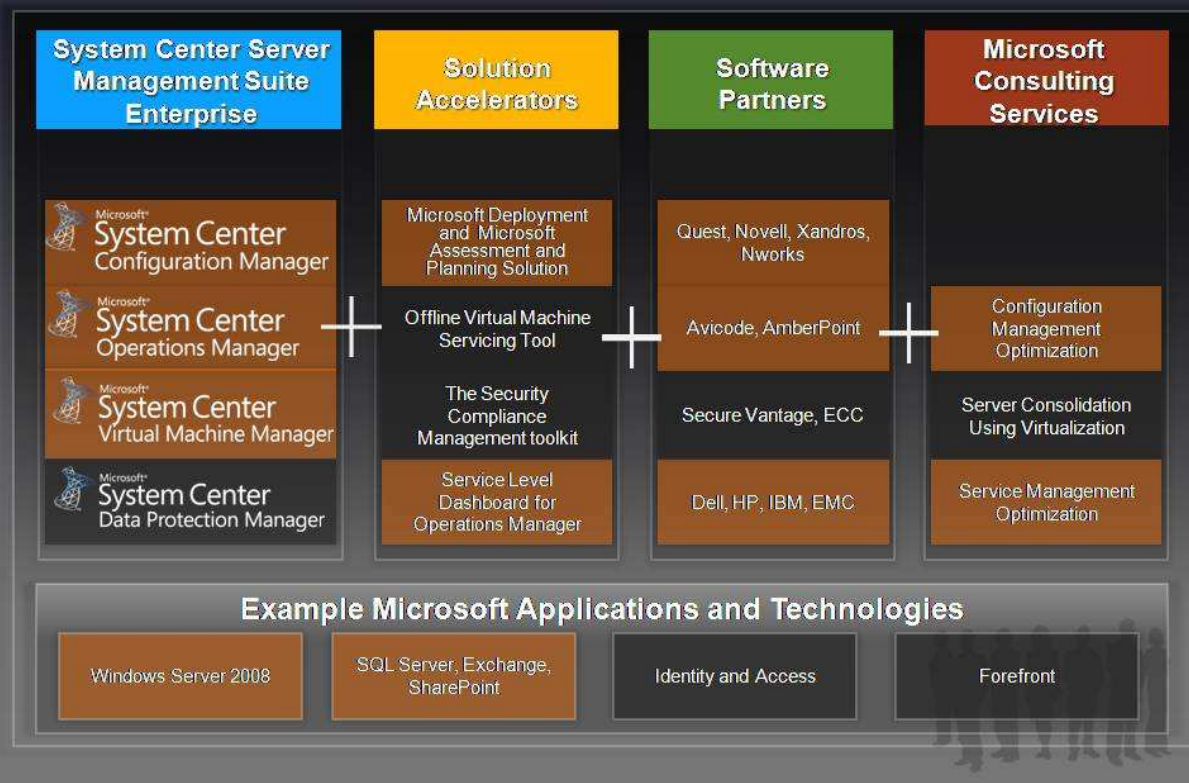
Server Management Suite Enterprise



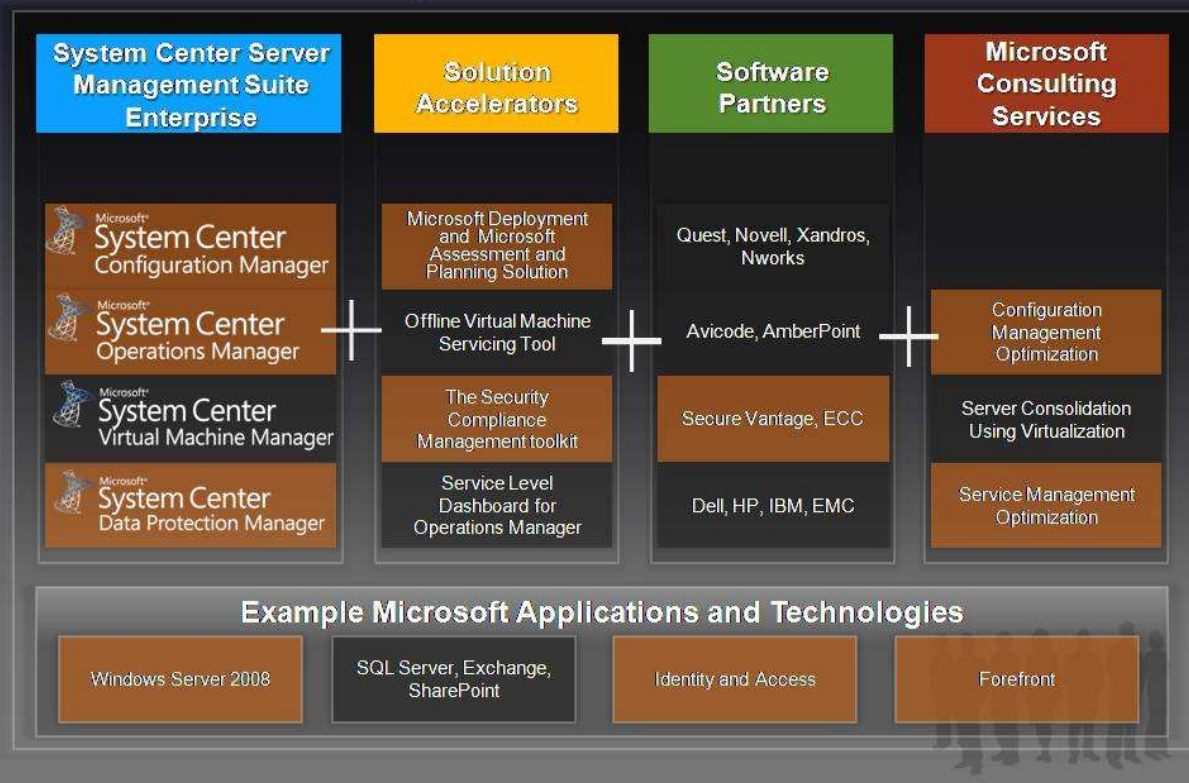
Microsoft®
System Center
Virtual Machine Manager



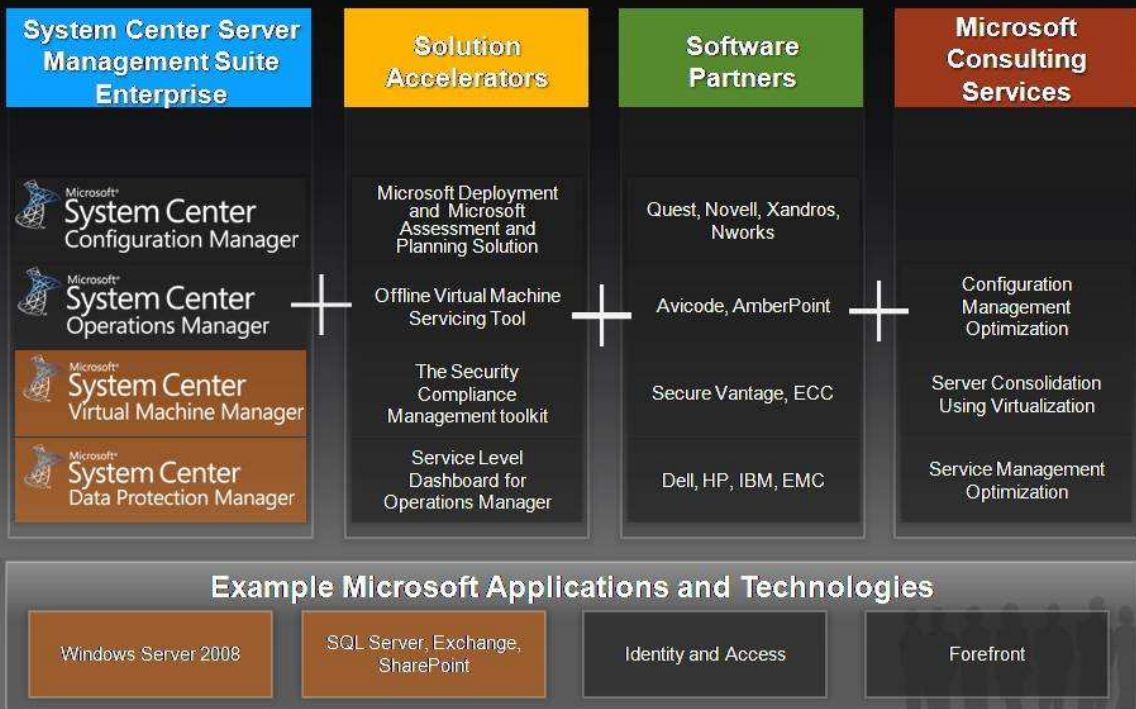
End to End Monitoring Solution



Server Compliance Solution



Data Protection and Recovery



Demo time....

Thanks you & Q-A



© 2008 Microsoft Corporation. All rights reserved.
This presentation is for informational purposes only. Microsoft makes no warranties, express or implied, in this summary.

Sơ lược tiểu sử Ông Vũ Nguyễn Cao Sơn:

Có nhiều năm công tác trong lĩnh vực công nghệ thông tin và tư vấn hệ thống. Hiện đang phụ trách chính về công nghệ hạ tầng, giải pháp an ninh cho nhóm khách hàng tài chính, tổng công ty tại khu vực phía Nam.

PHẦN 2: THÔNG TIN NHÀ TÀI TRỢ

1. Oracle



Oracle Vietnam

Hanoi Office

Unit 01 /02, 11th Floor, Prime Centre Building, 53 Quang Trung Street

Hanoi, Vietnam

Tel : +844 39446888

Fax : +844 39432 592

Ho Chi Minh Office

Suite 12 Sun Wah Business Centre

115 Nguyen Hue Boulevard, District 1

Ho Chi Minh City, Vietnam

Tel : +848 38219 186

Fax : + 848 38219 181

Oracle has been working in Vietnam since the lifting of the US trade embargo by President Clinton in February 1994. In 1995, Oracle Vietnam Pte Ltd. began operation as a 100% foreign owned subsidiary, and still is today, of Oracle Corporation (NASDAQ – ORCL)

Oracle was the first US information technology company to be granted such a license in Vietnam by the Government of Vietnam.

With a modern head office located in central Hanoi, Oracle Vietnam has been an instrumental leader in Vietnam's Information Technology modernization and a vocal advocate within the Vietnam Software Association of the continued need for software training and education.

To date, Oracle Vietnam has trained in excess of six thousand IT professionals and students in Vietnam and over three hundreds Vietnam IT experts have achieved the Oracle Certified Professional certification program.

As a direct result of these training programs, many of these professionals are now in demand not only in Vietnam but also throughout Asia, Europe and the United States.

Oracle Vietnam is capable of providing all products and services offered by Oracle worldwide including education and technical support for our partners and customers. Our technology products also support the Vietnamese language. Oracle is providing following solutions:

Oracle Database

Oracle Database, the first relational database designed for grid computing, helps ensure that enterprise information is always available and secure. Oracle is the most reliable choice for large enterprises, midsize businesses, and departments alike. Oracle provides the

- No. 1 Database
- No. 1 Data Warehousing
- No. 1 Database on Linux
- No. 1 Embedded Database

Oracle Fusion Middleware

Oracle Fusion Middleware consolidates Oracle's leading, standards-based software to deliver "hot-pluggable" middleware with a comprehensive and seamlessly integrated service-oriented architecture software infrastructure. Oracle is the

- No. 1 in Middleware
- No. 1 in Business Intelligence
- No. 1 in Application Platform suites
- No. 1 in Enterprise Performance Management

Oracle Applications

Oracle Applications—including Oracle E-Business Suite, PeopleSoft Enterprise, JD Edwards EnterpriseOne, JD Edwards World, Siebel, and Hyperion—help deliver the complete functionality and business intelligence that companies need to compete and win. In fact, Oracle has the No. 1 customer relationship management and human capital management applications, and benefits customers by enabling customer success, providing a complete offering, and presenting the strongest strategic road map.

Oracle Industry Solutions

Oracle industry solutions address the specific challenges and processes unique to your industry. Many of the world's top retail, manufacturing, life sciences, communications, utilities, and financial services firms are among the many businesses that are poised to profit from Oracle's industry focus. Globally, Oracle is a leader in financial services, the public sector, professional services, retail, and communications.

2. IBM Vietnam



IBM Việt Nam

Trụ sở chính: Tầng 2, Tòa nhà Pacific Place, 83B Lý Thường Kiệt, Quận Hoàn Kiếm, Hà Nội

ĐT: (84-4) 946 0201; Fax: (84-4) 946 0203

IBM Việt Nam

Chi nhánh tại HCMC: Tầng 3B, Trung Tâm Thương Mại Sài Gòn, 37 Tôn Đức Thắng, Quận 1, Thành Phố Hồ Chí Minh

ĐT: (84-8) 3824 1474; Fax: (84-8) 3822 5432

Website: www.ibm.com

Thành lập năm 1911 tại New York, Mỹ, IBM là tập đoàn công nghệ thông tin lớn nhất thế giới, cung cấp hàng loạt các giải pháp tích hợp, các sản phẩm dịch vụ công nghệ thông tin chất lượng vượt trội trên toàn cầu.

IBM trước đây đã có mặt ở Việt Nam từ năm 1938 đến năm 1975. Trở lại Việt Nam năm 1993, tới năm 1994, IBM thành lập hai văn phòng đại diện tại Hà Nội và Thành phố Hồ Chí Minh. Sau đó, Công ty IBM Việt Nam đã chính thức được thành lập và là một trong những doanh nghiệp 100% vốn nước ngoài đầu tiên trong ngành CNTT tại Việt Nam.

Tại Việt Nam, IBM cung cấp các sản phẩm và dịch vụ đa dạng bao gồm máy chủ (System x, System i, System p và System z), hệ thống lưu trữ (Storage), phần mềm (WebSphere, Information System – DB2, Lotus, Tivoli, Rational), các dịch vụ bảo hành, bảo dưỡng, tích hợp hệ thống, giải pháp e-business, quản lý dự án, giáo dục/đào tạo, và tư vấn.

Không ngừng đổi mới tất cả các chu trình và mô hình kinh doanh đã giúp cho IBM đạt những tầm cao mới về khả năng tích hợp các chu trình kinh doanh và các ứng dụng cho nội bộ doanh nghiệp, các nhà cung cấp, các nhà phân phối, khách hàng của doanh nghiệp và cho đội ngũ nhân viên. Khách hàng của IBM ở Việt Nam bao gồm các bộ, ngành, các cơ quan chính phủ, các ngân hàng, các doanh nghiệp quốc doanh, các công ty và tổ chức đa quốc gia hoạt động tại Việt Nam và các doanh nghiệp vừa và nhỏ.

IBM tự hào đóng góp vào quá trình phát triển của Việt Nam không chỉ bằng việc mang đến những giải pháp kinh doanh và trao đổi kinh nghiệm mà còn thông qua các dự án hỗ trợ giáo dục và văn hóa.

**IBM Vietnam Company**

2nd Floor, Pacific Place Building, 83B Ly Thuong Kiet Str., Hoan Kiem Dist., Hanoi, Vietnam

Tel: (84-4) 3946 0201

Fax: (84-4) 3946 0203

Website: www.ibm.com

IBM Vietnam Company

3B Floor, Saigon Trade Center, 37 Ton Duc Thang Street, District 1, Ho Chi Minh City,

Tel: (84-8) 3824 1474

Fax: (84-8) 3822 5432

Website: www.ibm.com

Established in 1911 in New York, United States, IBM is the world's leading information technology services company, offering a range of integrated solutions, products and services unmatched by any other IT company.

IBM set up its business and operated in Vietnam from 1938 to 1975. In 1993, IBM returned to Vietnam for market evaluation, and in 1994 established Representative Offices in Hanoi and Ho Chi Minh City. After that, IBM Vietnam Company was established and became one of the first 100% foreign-invested IT companies in Vietnam. IBM provides a complete range of products and services in Vietnam. These include servers (System x, System i, System p và System z), Storage System (TotalStorage), software (WebSphere, Information System – DB2, Lotus, Tivoli, Rational), Point-of-Sales systems, warranty/maintenance, system integration, e-business, project management, education/training, and consulting.

IBM's transformation across processes and enterprises, bring new levels of integration among processes and applications inside the business, suppliers and distributors at either end of the business, customers outside the enterprise, and employees inside it. Clients of IBM in Vietnam include government ministries and agencies, banks, state-owned enterprises, small- and medium-size enterprises and multi-national companies and organizations.

IBM is proud to contribute to the development and progress of Vietnam not only by providing unique business solutions, experience exchange but also through philanthropic projects to support the country's education and cultural renovation efforts.

3. HP



Tóm lược về HP năm 2008

Trong suốt 70 năm, HP đã giúp các cá nhân, doanh nghiệp, và cộng đồng trên khắp thế giới áp dụng công nghệ theo những cách mang đầy ý nghĩa bằng việc khai thác ý tưởng mới để cung cấp các sản phẩm và dịch vụ tin cậy. Các giải pháp của chúng tôi được dựa trên công nghệ mang tính trực giác ẩn giấu sự phức tạp bên trong, đúng chỗ của nó, để cuộc sống của khách hàng của chúng tôi cải thiện và trải nghiệm IT của họ đơn giản hơn, thông minh hơn và dễ quản lý hơn. Điều này cho phép họ ít phải lãng phí thời gian hơn để lo lắng về công nghệ và tập trung nhiều thời gian hơn vào những vấn đề chủ chốt.

Một số người nghĩ về HP như một công ty chuyên về máy in. Những người khác thì nghĩ về một công ty sản xuất máy tính, hoặc công ty chuyên về trung tâm dữ liệu. Chúng tôi chuyên về tất cả các thứ đó, và nhiều lĩnh vực khác:

- Chúng tôi phân phối trên 1 triệu máy in mỗi tuần.
- Chúng tôi phân phối 48 triệu đơn vị PC mỗi năm.
- Cứ ba máy chủ được phân phối trên toàn cầu thì có một là của HP.
- Phần mềm của HP giúp cho trên 100 triệu khách hàng sử dụng điện thoại di động trên khắp thế giới có thể thực hiện các cuộc gọi.
- HP giúp 50 triệu khách hàng lưu và chia sẻ trên 4 tỷ ảnh trực tuyến.
- HP hỗ trợ 200 ngân hàng hàng đầu và trên 130 sở giao dịch chứng khoán lớn trên thế giới.

Phục vụ các doanh nghiệp

Tại HP, chúng tôi liên tục khám phá cách công nghệ và các dịch vụ có thể tạo ra những phương thức mới và tốt hơn để mọi người sống, làm việc và giải trí. Hàng ngày, chúng tôi hợp tác với các khách hàng lớn nhất của chúng tôi để biến các môi trường IT hiện tại của họ thành những tài sản của doanh nghiệp. Chúng tôi nhận thấy rằng các CIO (Giám đốc Công nghệ Thông tin) bây giờ là những người quản lý doanh nghiệp chuyên về công nghệ. Chúng tôi cố gắng hết sức để giúp họ tạo ra những môi trường IT để quản lý hơn, có chi phí vận hành thấp hơn và cung cấp nhiều giá trị hơn cho doanh nghiệp. Điều đó có thể có nghĩa là kết hợp các cơ sở hạ tầng IT của họ, tăng tốc độ truy cập vào thông tin, cho phép giao tiếp nhanh hơn giữa các văn phòng chi nhánh và trụ sở chính, hoặc giúp họ xử lý những thiết bị IT lạc hậu. Các giải pháp của HP cân bằng danh mục rộng lớn của chúng tôi—from máy chủ tới phần mềm và các dịch vụ, hình ảnh và in ấn, cũng như công nghệ máy tính cá nhân—để giúp các công ty thúc đẩy sự phát triển, giảm rủi ro trong kinh doanh, và cắt giảm chi phí.

Phục vụ các doanh nghiệp vừa và nhỏ

HP cũng đang làm thay đổi cách làm việc của các doanh nghiệp vừa và nhỏ. Chúng tôi giúp các doanh nghiệp kết nối với khách hàng và tăng thu nhập bằng các giải pháp đã được kiểm chứng cho di động, bảo mật, bảo vệ công việc kinh doanh, và điểm bán hàng. Với hàng loạt các sản phẩm và dịch vụ in ấn cũng như hình ảnh, HP giúp các công ty này nổi bật và giảm chi phí in ấn chung bằng cách giúp họ tự in các tài liệu tiếp thị có số lượng ít. Với các ưu đãi trực tuyến và tại cửa hàng của HP từ Logoworks bởi HP, các doanh nghiệp nhỏ có thể truy cập vào mạng lưới các nhà thiết kế chuyên nghiệp và các đối tác bán lẻ để giúp xây dựng thương hiệu của họ.

Ngoài ra, với các giải pháp của HP, các doanh nghiệp vừa và nhỏ còn nhận được nhiều hơn là chỉ công nghệ tuyệt vời—they có được Sự Chăm Sóc Toàn Diện của HP. Danh mục dịch vụ và hỗ trợ rộng lớn của chúng tôi giúp họ sử dụng, bảo vệ và tái chế các sản phẩm của họ. Điều đó, kết hợp với khả năng truy cập dễ dàng vào sự phân phối và kỹ năng chuyên môn của các đối tác địa phương, cho phép họ tập trung vào những vấn đề chủ chốt, đó là tình hình phát triển của doanh nghiệp của họ.

Phục vụ người tiêu dùng

Người tiêu dùng trên khắp thế giới muốn dễ dàng truy cập vào thông tin, dịch vụ giải trí, dịch vụ kỹ thuật số và chia sẻ chúng với người khác. HP áp dụng công nghệ để làm cho những trải nghiệm này đơn giản hơn và đồng thời bổ ích hơn.

Điều đó có nghĩa là giúp mọi người dễ dàng in, lưu trữ và chia sẻ ảnh kỹ thuật số của họ. Với công nghệ HP, người tiêu dùng có thể tự thể hiện mình bằng những bức ảnh, áp phích, và sách ghi nhớ giàu tưởng tượng có chất lượng cao và bền được tạo tại nhà bằng cách sử dụng máy Photosmart có nhiều chủng loại để lựa chọn, trực tuyến thông qua Snapfish của HP, hoặc tại cửa hàng bán lẻ trong vùng của họ.

Chúng tôi giúp người tiêu dùng có thể có được một phong cách sống độ phân giải cao một cách dễ dàng và đơn giản hơn. Đó là lý do vì sao chúng tôi đã phát triển những sản phẩm như là HP MediaSmart Connect và HP MediaSmart Server. HP MediaSmart Connect là một bộ nhận phương tiện kỹ thuật số hiện đại có thể biến bất kỳ tivi có độ phân giải cao (HDTV) nào thành một tivi được kết nối của thế hệ tương lai, cho phép người tiêu dùng thưởng thức ảnh, nhạc, phim và video ưa thích—có dây hoặc không dây—from nhiều PC quanh nhà trên "màn hình lớn" trong trái tim của nhà. Ngoài ra, HP MediaSmart Server của chúng tôi cho phép người tiêu dùng kết nối với nhiều máy tính trong nhà và sao lưu, truy cập, cũng như chia sẻ các tệp của chúng từ một vị trí tập trung.

Thúc đẩy sự chuyển đổi công nghệ

Với lượng dữ liệu ngày nay tăng nhanh hơn khả năng nắm giữ và sử dụng chúng của chúng ta, ngành công nghiệp nhanh chóng chuyển sang mô hình mà mọi thứ có thể được cung cấp như một dịch vụ. Mọi người muốn truy cập ngay tức thì vào nội dung và thông tin mà họ quan tâm. Việc đáp ứng nhu cầu trên toàn cầu về thông tin và nội dung giàu kỹ thuật số sẽ đòi hỏi các dịch vụ linh hoạt, hấp dẫn. Các khối xây dựng cơ bản của mô hình này sẽ là các mạng thông minh hơn, giàu trí tuệ hơn; các trung tâm dữ liệu thể hệ tương lai; và quan trọng nhất có thể là phần mềm kết hợp tất cả những thành phần hỗn tạp lại với nhau.

Trong năm năm tới, HP sẽ đầu tư 20 tỷ đô la vào R&D (nghiên cứu & phát triển) xoay quanh ba lĩnh vực công nghệ mà chúng tôi tin là có khả năng thúc đẩy ngành này phát triển và cải thiện cách khách hàng của chúng tôi sống và làm việc.

- Trước tiên là việc giúp đỡ các khách hàng doanh nghiệp chuyển đổi môi trường IT của họ thành các trung tâm dữ liệu được trừu tượng hóa, có tính tự động cao, để giảm đáng kể chi phí bảo dưỡng và vận hành trong khi vẫn tăng sự nhanh nhẹn, công suất tính toán, và khả năng lưu trữ dữ liệu.
- Thứ hai là nâng cấp cơ sở hạ tầng, mạng, và thiết bị để tạo những trải nghiệm máy tính được cá nhân hóa cao hơn, đơn giản hơn để mọi người có thể dễ dàng truy cập vào và chia sẻ nội dung và các dịch vụ quan trọng nhất đối với họ trên mọi thiết bị, từ bất kỳ vị trí nào, vào bất kỳ lúc nào.
- Thứ ba là chuyển đổi cách nội dung được tạo và sử dụng cả về mặt thực tế và kỹ thuật số, điều này sẽ cách mạng hóa cách công bố như chúng ta đã biết. Với các doanh nghiệp, điều này sẽ tạo ra các cơ hội để sáng tạo ra những dịch vụ mới, phong phú và tạo ra những mô hình kinh doanh và những nguồn thu nhập mới. Người tiêu dùng sẽ linh hoạt hơn trong việc truy cập vào và công bố nội dung của họ một cách đơn giản và dễ dàng hơn.

Người tiên phong trong công nghệ

Việc xây dựng những kiểu trải nghiệm này đòi hỏi chuyên môn và sự sáng tạo trên khắp các thiết bị, cơ sở hạ tầng, và các dịch vụ làm cho có thể. HP cung cấp một danh mục độc đáo để giúp khách hàng của chúng tôi áp dụng công nghệ để làm bất cứ những gì họ muốn làm:

- **Các hệ thống cá nhân**—HP có một danh mục hàng đầu gồm các PC dành cho doanh nghiệp và người tiêu dùng, các máy trạm hiệu suất cao, các thiết bị cầm tay, các giải pháp giải trí kỹ thuật số, thiết bị lưu trữ cá nhân, và các dịch vụ Internet tạo ra những trải nghiệm kết nối và hấp dẫn.
- **Hình ảnh và in ấn**—HP dẫn đầu trong việc chuyển đổi kỹ thuật số việc in ấn và cung cấp cho các khách hàng của mình những cách mới hấp dẫn để sáng tạo, tiết kiệm tiền, cải thiện năng suất, và nổi trội. Với các thị trường gia đình, văn phòng và đồ họa, HP có hàng loạt các sản phẩm và dịch vụ đã giành được giải thưởng để giúp khách hàng của chúng tôi thành công.

- **Các giải pháp công nghệ**—HP cung cấp hàng loạt các giải pháp tập trung vào việc giúp đỡ các khách hàng doanh nghiệp của chúng tôi quản lý và chuyển đổi môi trường công nghệ của họ để có được kết quả kinh doanh tốt hơn. Các khách hàng doanh nghiệp có thể tận dụng công nghệ và chuyên môn của chúng tôi bằng cách cân bằng các khối xây dựng cốt lõi của chúng tôi—máy chủ và lưu trữ, phần mềm, và dịch vụ.

- **Các dịch vụ của HP**—Là một đối tác kết nối toàn cầu tin cậy, chúng tôi tập trung vào việc giải quyết những thách thức của khách hàng bằng những đổi mới thiết thực giúp tạo ra kết quả kinh doanh có giá trị. Việc mua lại EDS gần đây đã làm cho HP trở thành công ty dịch vụ công nghệ lớn thứ hai trên thế giới—với 210.000 nhân viên dịch vụ và phòng nghiệp vụ tại 80 quốc gia. Sự kết hợp mạnh mẽ giữa nguồn lực và tài năng này tạo cho chúng tôi qui mô và phạm vi để quản lý những nhu cầu công nghệ kinh doanh quan trọng nhất của khách hàng.

- **Các Dịch vụ Tài chính của HP** giúp khách hàng hướng tới tổng chi phí sở hữu thấp nhất trong suốt vòng đời của công nghệ—từ lập kế hoạch và mua công nghệ suốt cho tới cho nghĩ và thay thế nó. Chúng tôi giúp họ triển khai công nghệ kinh doanh tâm cơ thể giới một cách dễ dàng và kinh tế nhờ đáp ứng các nhu cầu riêng của họ.

- **Các Phòng thí nghiệm của HP**—Các nhóm thăm dò và nghiên cứu nâng cao của chúng tôi mở rộng lĩnh vực khoa học cơ bản. Với 23 phòng thí nghiệm tại 7 vị trí trên khắp thế giới, các Phòng thí nghiệm của HP tập trung vào nghiên cứu có tầm ảnh hưởng lớn để giải quyết những thách thức phức tạp nhất mà những khách hàng công nghệ sẽ phải đối mặt trong thập niên tới trong các lĩnh vực khám phá thông tin, các dịch vụ máy động, chuyển đổi nội dung, cơ sở hạ tầng thông minh, và sự bền vững.

Tư cách công dân toàn cầu

Tư cách công dân toàn cầu là cam kết của HP để đưa bản thân chúng tôi lên thành người làm chính, minh bạch, và trách nhiệm cao hơn. Các giá trị đã có kể từ khi HP được thành lập năm 1939 vẫn không thể thiếu trong công việc của chúng tôi ngày hôm nay, giúp chúng tôi cân bằng các mục tiêu kinh doanh với ảnh hưởng của chúng tôi lên xã hội và hành tinh.

Chúng tôi có ba lĩnh vực ưu tiên trong tư cách công dân toàn cầu: nâng cao tiêu chuẩn về xã hội và môi trường trong chuỗi cung cấp của chúng tôi, cải thiện hiệu suất năng lượng của các hoạt động và sản phẩm của chúng tôi để giảm tác động của chúng lên môi trường, và khuyến khích tái sử dụng và tái chế sản phẩm nhiều hơn.

Nỗ lực của chúng tôi trong các lĩnh vực này giúp tạo ra cho HP sự khác biệt, giảm chi phí, và thúc đẩy sáng tạo khi chúng tôi đáp lại các cơ hội thị trường ngày một phát triển và kỳ vọng của các cổ đông.

Chúng tôi tiếp tục tập trung vào việc cải thiện cuộc sống của các cá nhân và cộng đồng trên khắp thế giới, phần đầu tác động tạo ra thay đổi tích cực và bền lâu. Tại HP, việc rèn luyện tư cách công dân toàn cầu tốt bao gồm sự ủng hộ quyền con người và quyền lao động, đầu tư xã hội chiến lược—cụ thể là nâng cao thành quả của sinh viên và sự thành công của các doanh nghiệp mới, và bảo vệ quyền riêng tư của khách hàng và thông tin của nhân viên.

Tóm lược

HP tập trung vào việc đơn giản hóa các trải nghiệm công nghệ cho tất cả các khách hàng của mình—từ người tiêu dùng cá nhân cho tới những doanh nghiệp lớn nhất. Với một danh mục trải rộng trong các lĩnh vực in ấn, máy tính cá nhân, phần mềm, dịch vụ và cơ sở hạ tầng IT, thu nhập của HP đạt 118,4 tỷ đô la trong bốn quý tài chính kết thúc vào ngày 31 tháng 10 năm 2008. Trụ sở của công ty đặt tại Palo Alto, California, nhưng công ty thực sự là một tập thể toàn cầu, với 320.000 nhân viên làm việc tại trên 170 quốc gia trên khắp thế giới, và 69% thu nhập của công ty là từ bên ngoài Hoa Kỳ. Mark Hurd là chủ tịch đương nhiệm của chúng tôi đồng thời là tổng giám đốc.

HP là một công ty hàng đầu trên thế giới về số thị trường:

- Số 1 về máy in LaserJet và inkjet*
- Số 1 về máy chủ Windows®, Windows, UNIX®, và Linux*
- Số 1 về máy tính xách tay và máy tính để bàn*
- Số 2 thế giới về máy trạm
- Số 1 về máy chủ blade*
- Đứng thứ 1 về hệ thống lưu trữ đĩa toàn diện*
- Số 1 thế giới về phần mềm quản lý hệ thống được phân phối*
- Số 1 thế giới về chất lượng phần mềm tự động*
- Số 2 thế giới về dịch vụ IT**

www.hp.com

*Dữ liệu toàn cầu quý 3 năm 2008 của IDC

**IDC; Thị phần Toàn cầu về Số liệu Thị trường Dịch vụ IT tháng 4 năm 2008 của Gartner

© Bản quyền 2008 Hewlett-Packard Development Company, L.P. Thông tin có trong tài liệu này có thể thay đổi mà không cần thông báo trước. HP sẽ không chịu trách nhiệm pháp lý đối với các lỗi hoặc sai sót kỹ thuật hoặc biến tập ở trong tài liệu này. Windows là nhãn hiệu đã đăng ký tại Hoa Kỳ của Microsoft Corporation. UNIX là nhãn hiệu đã đăng ký của The Open Group.

4AA0-8427VIVN Rev. 3, tháng 10 năm 2008



4. Cisco



Cisco Systems, Inc. là công ty hàng đầu thế giới về kết nối mạng Internet. Hiện nay, mạng là một bộ phận quan trọng trong hoạt động liên lạc của các doanh nghiệp, trường học, cơ quan chính phủ và hộ gia đình, và các giải pháp mạng dựa trên giao thức IP (Internet Protocol) của Cisco lại chính là nền tảng của những mạng này.

Cisco được thành lập năm 1984 bởi một nhóm các nhà khoa học máy tính tại Trường Đại học Stanford. Kể từ khi thành lập, các kỹ sư của Cisco luôn là những người đi tiên phong trong việc phát triển các công nghệ mạng dựa trên giao thức IP. Hiện nay, với hơn 54,000 nhân viên trên toàn thế giới, truyền thống sáng tạo được tiếp nối với những sản phẩm và giải pháp hàng đầu thị trường trong các lĩnh vực phát triển cốt lõi của công ty là định tuyến và chuyển mạch, cũng như là trong các lĩnh vực công nghệ tiên tiến như:

- ☐ Truyền thông IP
- ☐ Mạng LAN không dây
- ☐ Kết nối mạng gia đình
- ☐ Các dịch vụ kết nối ứng dụng
- ☐ An ninh mạng
- ☐ Kết nối mạng lưu trữ
- ☐ Các hệ thống Video

Cisco nằm ở tâm điểm của nhiều thay đổi mang tính lịch sử về công nghệ, và điều đó vẫn tiếp tục đúng cho đến tận thời điểm hiện nay. Giờ đây, khi mà lĩnh vực công nghệ đang trải qua một giai đoạn thay đổi căn bản, Cisco vẫn là công ty hàng đầu thị trường trong rất nhiều lĩnh vực như là định tuyến và chuyển mạch, truyền thông hợp nhất, truyền thông không dây và an ninh. Công ty đã giúp thúc đẩy sự chuyển dịch của cả ngành công nghiệp hướng đến IP và giờ đây Cisco cũng đang nằm ở tâm điểm của những thay đổi căn bản trong cách thức truyền thông của cả thế giới.

Mạng như là Nền tảng

Sự xuất hiện của khái niệm Mạng như là Nền tảng (the network as a platform) đang làm thay đổi toàn bộ chuỗi giá trị của công nghệ và đặt mạng lưới vào trung tâm của sáng tạo: tới năm 2010, sẽ có đến 14 tỷ thiết bị được kết nối vào mạng Internet. Sự bùng nổ về số lượng thiết bị sẽ còn được tăng cường thêm nữa khi ngày càng có nhiều dịch vụ và công việc được xử lý trực tuyến, từ các cuộc gọi điện thoại cho đến tìm kiếm cá nhân hay tải video, game và các hình thức giải trí khác nữa.

Vai trò của mạng lưới đang phát triển vượt quá việc chỉ đơn thuần là một cơ sở hạ tầng. Nó đang nổi lên như là một nền tảng an toàn để cung cấp những trải nghiệm mang tính tùy biến và cá nhân hóa mà những người dùng của thế kỷ 21 kỳ vọng, dù đó là cung cấp các dịch vụ mới như là một nhà khai thác, nâng cao năng suất của doanh nghiệp ở mọi quy mô hoặc là người tiêu dùng đang tìm kiếm những hoạt động giải trí và dịch vụ theo thời gian thực được cá nhân hóa.

Khi mà một mạng lưới ngày càng thông minh phát triển thành một nền tảng, người dùng sẽ có thể liên lạc từ bất kỳ thiết bị nào, theo bất cứ chế độ nào mà họ lựa chọn.

Cisco đang lãnh đạo sự chuyển đổi hướng đến một môi trường công nghệ lấy mạng lưới làm trung tâm. Bằng cách kết hợp thế mạnh cốt lõi của mình (IP) với trí tuệ, công ty đang tạo ra một nền tảng truyền thông mạnh mẽ đóng vai trò cơ sở cho sự hội tụ của dữ liệu, thoại, video và truyền thông di động vào trong một kiến trúc tích hợp, an toàn.

Nghiên cứu và Phát triển

Để biết thêm thông tin, vui lòng liên hệ:

**Cisco Systems
Vietnam**

**Level 12A, Vincom
City Towers, 191 Ba
Triệu, Hanoi.**

Tel: 84.4. 39746 227

Fax: 84.4. 39742 790

www.Cisco.com/vn

Cisco sáng tạo theo rất nhiều cách thức: thông qua phát triển công nghệ và mở rộng các công nghệ sau khi chúng được phát minh ra cũng như thông qua những công nghệ tương tự và mở rộng thị trường. Chúng tôi còn sáng tạo thông qua sự tích hợp ở đẳng cấp thế giới và mở rộng hoạt động mua lại công ty, thông qua triển khai những mô hình kinh doanh mới và thông qua cách chúng tôi hợp tác với các công ty khác.

Chương trình Học viện Mạng của Cisco

Để giúp nâng cao khả năng tiếp cận đến các cơ hội đào tạo và nghề nghiệp trên toàn thế giới, Cisco đã xây dựng Chương trình Học viện Mạng của Cisco (Cisco Networking Academy Program) để đào tạo sinh viên trong việc thiết kế, xây dựng và duy trì các mạng máy tính. Bằng cách kết hợp giữa đào tạo và mạng Internet, Chương trình Học viện Mạng của Cisco giúp sinh viên thu nhận những kỹ năng cần thiết cho các công việc trong lĩnh vực IT và hỗ trợ hoạt động đào tạo đại học trong lĩnh vực kỹ thuật, khoa học máy tính và những lĩnh vực khác có liên quan – và cuối cùng là hỗ trợ việc phát triển các quốc gia và nền kinh tế của các quốc gia đó. Kể từ khi ra đời vào năm 1997, đã có hơn 1.6 triệu sinh viên theo học tại hơn 10,000 Học viện Mạng được đặt tại các trường trung học, các trường kỹ thuật, cao đẳng, đại học và các tổ chức đào tạo cộng đồng ở hơn 163 quốc gia trên thế giới.

Các Đối tác Kênh hỗ trợ sự Phát triển Mạng

Công nghệ mạng đang nhanh chóng thay đổi và tạo ra những nhu cầu mới cho các doanh nghiệp và tổ chức ở mọi thể loại. Để đáp ứng, Cisco Systems đã phát triển một chương trình đối tác kênh hàng đầu để hỗ trợ đội ngũ bán hàng là các đối tác kênh hết sức quan trọng của công ty phát triển các kỹ năng và kiến thức chuyên môn mà họ cần có để phát triển.

Các Đối tác Kênh của Cisco (Cisco's channel partners), một lực lượng toàn cầu với hơn 200,000 người thuộc hơn 20,000 nhà bán lẻ, nhà tích hợp hệ thống và nhà tư vấn mạng gia tăng giá trị đang chiếm tới hơn 90% doanh thu thương mại và doanh nghiệp trên toàn cầu của Cisco.

Để biết thêm thông tin về Cisco và các chương trình công nghệ của công ty, vui lòng ghé thăm: www.Cisco.com.



Cisco Systems, Inc. is the worldwide leader in networking for the Internet. Today, networks are an essential part of business, education, government and home communications, and Cisco's Internet Protocol-based (IP) networking solutions are the foundation of these networks.

Cisco was founded in 1984 by a small group of computer scientists from Stanford University. Since the company's inception, Cisco engineers have been leaders in the development of Internet Protocol (IP)-based networking technologies. Today, with more than 54,000 employees worldwide, this tradition of innovation continues with industry-leading products and solutions in the company's core development areas of routing and switching, as well as in advanced technologies such as:

- ☐ IP Communications
- ☐ Home Networking
- ☐ Network Security
- ☐ Video Systems
- ☐ Wireless LAN
- ☐ Application Networking Services
- ☐ Storage Area Networking

Cisco has been at the heart of many historic changes in technology, and that continues to be true today. Now, at a time when the technology industry is going through a period of dramatic change, Cisco is the market leader in multiple areas, such as routing and switching, unified communications, wireless and security. The company helped catalyze the industry's move toward IP and, now that it is fully underway, the company is at the center of fundamental changes in the way the world communicates.

The Network is the Platform

The emergence of the network as a platform is changing the entire value chain of technology and placing the network squarely at the center of innovation: as many as 14 billion devices will be connected to the Internet by 2010. The explosion of devices will be fueled by more and more services and tasks being handled online, from phone calls to personalized searches to downloading videos, games and other forms of entertainment.

The role of the network is evolving beyond that of infrastructure. It is emerging as a secure platform for delivering the customized and personalized experience that 21st century users expect - whether that means delivering new services as a carrier, boosting productivity for businesses of any size or consumers looking for real-time, personalized entertainment and services.

As an increasingly intelligent network evolves into a platform, users will be able to communicate from any device and in whatever mode they choose.

Cisco is leading the transition to a network-centric technology environment. By combining its core strength (IP) with intelligence, the company is creating a powerful communications platform that will serve as the basis for the convergence of data, voice, video and mobile communications in a secure, integrated architecture.

Research and Development

Cisco innovates in many different ways: via technology development and the expansion of technologies after their initial invention, and through adjacent technology and market extension. We also innovate through world-class integration and scaling of acquisitions, by starting new business models, and in the way we partner with other companies.

For more information,
please contact:

Cisco Systems Vietnam

**Level 12A, Vincom City
Towers, 191 Ba Trieu,
Hanoi.**

Tel: 84.4. 39746 227

Fax: 84.4. 39742 790

www.Cisco.com/vn

Cisco Networking Academy Program

To help foster access to education and professional opportunities worldwide, the company founded the Cisco Networking Academy Program, which trains students to design, build, and maintain computer networks. By combining education and the Internet, Cisco Networking Academies help students acquire the skills needed for IT-related jobs and for higher education in engineering, computer science, and related fields—and ultimately, aid in the development of their countries and their local economies. Since its creation in 1997, over 1.6 Million students have enrolled at more than 10,000 Academies located in high schools, technical schools, colleges, universities, and community-based organizations in more than 163 countries.

Channel Partners Address Network Evolution

Network technology is rapidly changing and creating new demands by businesses and organizations of all types. In response, Cisco Systems has developed its industry-leading channel partner program to help the company's important sales force, its channel partners, develop the skills and expertise they need to thrive.

Cisco's channel partners, a global force of over 200,000 people in 20,000 independent value-added resellers, systems integrators and network consultancies, account for more than 90 percent of Cisco's commercial and enterprise revenue worldwide.

For more information on Cisco and its technology initiatives, go to www.Cisco.com.

5. Microsoft

Microsoft (đôi khi viết tắt là **MS**) là một tập đoàn Công nghệ máy tính đa quốc gia tầm cỡ thế giới của Mỹ do Bill Gates làm chủ tịch, với số nhân viên là 79.000 người tại 102 quốc gia và tổng doanh thu năm 2007 đạt 51,12 tỷ USD. Tập đoàn này phát triển, gia công, và cấp bản quyền cho các phần mềm phục vụ trong máy tính. Trụ sở chính của Microsoft đặt tại Redmond, Washington Mỹ.

Các sản phẩm bán chạy nhất của Microsoft bao gồm họ các hệ điều hành thuộc họ Microsoft Windows (Windows NT, Windows 95, Windows 98 SE, Windows ME, Windows 2000, Windows XP (SP1, SP2), Windows Server 2003, Windows Vista) và bộ phần mềm văn phòng Microsoft Office. Đó là những sản phẩm rất nổi tiếng trong thị trường phần mềm cho máy tính cá nhân, chiếm thị phần lên đến 90% hoặc hơn như với Microsoft Office năm 2003, và Microsoft Windows năm 2006.

Được thành lập để phát triển phần mềm trình dịch BASIC interpreters cho máy Altair 8800, Microsoft vươn lên thống trị thị trường hệ điều hành cho máy tính gia đình với MS-DOS giữa những năm 1980. Cổ phiếu của công ty sau khi được phát hành lần đầu ra thị trường đã tăng giá nhanh chóng và tạo ra 4 nhà tỷ phú và 12000 nhà triệu phú trong công ty. Xuyên suốt lịch sử, tập đoàn này luôn là mục tiêu của rất nhiều sự chỉ trích, bao gồm các thủ đoạn độc quyền kinh doanh. Trong đó có từ phía Ủy ban công lý Hoa Kỳ (United States Department of Justice), và Ủy ban châu Âu (*European commission*), đã làm Microsoft dính vào rất nhiều vụ kiện tụng về chống độc quyền.

Microsoft cũng có một chỗ đứng trong các thị trường khác bên cạnh thị trường hệ điều hành và phần mềm văn phòng, như mạng truyền hình cáp MSNBC, cổng Internet MSN, và bộ từ điển bách khoa đa phương tiện Microsoft Encarta. Công ty cũng kinh doanh hai dòng sản phẩm phần cứng máy tính là Microsoft mouse và sản phẩm giải trí gia đình như Xbox, Xbox 360, Zune và MSN TV.

Windows Live (Bản Beta) mới được công bố ở trang <http://www.ideas.live.com/> và sắp tới là hệ điều hành Windows Vista, bản Microsoft Office 2007 dự kiến tới cuối năm 2006, đầu năm 2007 sẽ phát hành và công bố rộng rãi trên toàn cầu. Sản phẩm văn phòng Microsoft Office (95, 97, 2000, XP, 2003, 2007).

Lịch sử

- 6/1978: Bill Gates và Paul Allen đăng ký bản quyền cho sản phẩm trí tuệ đầu tay và **tháng 11/1978 Microsoft chính thức được ra đời.**

Phạm vi hoạt động

Microsoft có mặt tại hầu hết các quốc gia và, Microsoft đặt chi nhánh ở hơn 102 quốc gia (2007) và được phân loại thành 6 khu vực:

1. Bắc Mỹ.
2. Châu Mỹ Latinh.
3. Châu Âu, Trung Đông, Châu Phi.
4. Nhật Bản.
5. Châu Á Thái Bình Dương.
6. Trung Quốc.

6. BUREAU VERITAS

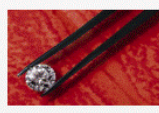


DỊCH VỤ CHỨNG NHẬN

► Có mặt trên 140 quốc gia, 40 Công nhận, cấp trên 80 000 giấy chứng nhận trên thế giới, trong đó >2.000 giấy chứng nhận được cấp cho các doanh nghiệp tại Việt Nam

- Chứng nhận hệ thống
 - Quản lý chất lượng (ISO 9000)
 - Quản lý môi trường (ISO 14000, EMAS)
 - Quản lý chất lượng trong ngành công nghiệp ô tô (VDA6.1, TS 16949)
 - Thực phẩm (HACCP, EUREPGAP, BRC, ISO 22000)
 - Viễn thông (TL 9000)
 - Thiết bị y tế (EN 46000)
- An toàn (Safetycert®, OHSAS 18001, VCA, BS 8800)
 - Trách nhiệm xã hội SA 8000
 - Đạo đức kinh doanh
- Công nghệ thông tin (TickIT, BS 7799, ISO 17799, **ISO 27001**)
- Đánh giá sự phù hợp, so sánh chuẩn các hệ thống
 - Chứng nhận cấp độ của HTQL theo VeriCERT
 - Chứng nhận cấp độ an toàn theo **VeriSAFE**
 - Chứng nhận sản phẩm (Dấu CE cho thiết bị y tế; Thiết bị áp lực theo tiêu chuẩn EU)






Bureau Veritas Certification Vietnam ISMS trong Ngày An toàn Thông tin – 18 November 2008

DỊCH VỤ ĐÀO TẠO

► Chất lượng

- ISO 9000:
ISO/TS 16949: Đào tạo nhận thức và đào tạo đánh giá viên nội bộ
Đào tạo chuyên gia đánh giá trường có đăng ký IRCA
Đào tạo đánh giá viên nội bộ năng cao

► Môi trường

- ISO 14000:
Đào tạo chuyển đổi hệ thống
ISO 14001:2004
Đào tạo đánh giá viên nội bộ
Đào tạo chuyên gia đánh giá trường có đăng ký IRCA

► Các công cụ cải tiến sau chứng nhận

- 5 Công cụ
 - SPC và ứng dụng
 - MSA, FMEA, APQP, PPAP
- 6 Sigma:
 - Nhận thức 6 sigma
 - Green Belts

► OH&S

- Safety Cert,
- OHSAS 18000:
 - Đào tạo đánh giá viên hệ thống

► Thực Phẩm

- HACCP (Nhận thức, ĐG Nội bộ)
- ISO 22000 (Nhận thức, ĐG Nội bộ)
- Đào tạo chuyên gia đánh giá trường có đăng ký IRCA

► Hệ thống tích hợp



- VeriCERT: Bureau Veritas Certification Vietnam ISMS trong Ngày An toàn Thông tin – 18 November 2008

3

ĐƯỢC CÔNG NHẬN

Công nhận quốc tế → Thừa nhận toàn cầu

HOA KỲ



VƯƠNG QUỐC ANH



TỔ CHỨC TRÁCH NHIỆM XÃ HỘI QUỐC TẾ



ĐÀO TẠO



Công nhận quốc tế → Chứng nhận chuyên ngành

RC 14001/RCMS



SFI



FOOD – IFS



TS 16949



PEFC



FSC



FOOD – EUREPGAP



TAPA



Bureau Veritas Certification Vietnam ISMS trong Ngày An toàn Thông tin – 18 November 2008

4

ĐƯỢC CÔNG NHẬN

Công nhận quốc gia → Thừa nhận quốc tế



Bureau Veritas Certification Vietnam ISMS trong Ngày An toàn Thông tin – 18 November 2008

5

BUREAU VERITAS CERTIFICATION VIETNAM

- ▶ Phát hành 2000 Giấy chứng nhận phù hợp với các tiêu chuẩn quốc tế cho các HTQL
- ▶ Phù hợp ISO 17021:2006 & được chuyển thành Trung tâm chứng nhận (ICC) từ tháng 9 năm 2008
 - Quyết định chứng nhận với công nhận của UKAS & ANAB.
 - Kịp thời hơn với nhu cầu khách hàng
- ▶ Có chuyên gia đánh giá người Việt Nam
- ▶ Khách hàng tiêu biểu tại Việt Nam ISO 27001:2005–UKAS công nhận
 - YKK.
 - BKIS



Bureau Veritas Certification Vietnam ISMS trong Ngày An toàn Thông tin – 18 November 2008

6



Move Forward with Confidence

Any request or information, please contact: **Ms. Nguyen Mỹ Hạnh**

Tel.: 8 122 246 Ext. 128 or E-mail: my-hanh.nguyen@vn.bureauveritas.com

Thank you!

Bureau Veritas Certification Vietnam ISMS trong Ngày An toàn Thông tin – 18 November 2008

7

7. TRUSTBank



Ngân hàng thương mại cổ phần (TMCP) Đại Tín – TRUSTBank chính thức thành lập vào năm 1989, với tên gọi là Ngân hàng TMCP nông thôn Rạch Kiến - ngân hàng cổ phần đầu tiên của tỉnh Long An, và được Ngân

hàng Nhà nước Việt Nam cấp giấy phép hoạt động số 0047/NH-GP ngày 29/12/1993, trụ sở chính tại số 1, Thị tứ Long Hòa, Huyện Cần Đước, Tỉnh Long An.

Ngày 17/08/2007, theo quyết định số 1931/QĐ-NHNN, Ngân hàng TMCP nông thôn Rạch Kiến được Thống đốc NHNN Việt Nam chấp thuận chính thức chuyển đổi mô hình hoạt động thành Ngân hàng TMCP đô thị và đổi tên thành Ngân hàng TMCP Đại Tín, theo quyết định số 2136/QĐ-NHNN ngày 17/09/2007 của NHNN Việt Nam.

Việc chấp thuận cho TRUSTBank chuyển đổi mô hình hoạt động từ Ngân hàng TMCP nông thôn sang Ngân hàng TMCP đô thị tạo điều kiện cho NH nâng cao năng lực về tài chính, mở rộng mạng lưới hoạt động kinh doanh, đủ sức cạnh tranh và phát triển mạnh mẽ, đánh dấu một giai đoạn phát triển mới của TRUSTBank với mục tiêu phấn đấu trở thành một ngân hàng bán lẻ hiện đại theo các chuẩn mực quốc tế, cung cấp sản phẩm dịch vụ đa dạng từ cơ bản đến cao cấp, hoàn thành mục tiêu đưa TRUSTBank trở thành một trong số các ngân hàng có chất lượng phục vụ tốt nhất tại Việt Nam.

I - Vốn điều lệ:

Tính đến 13/11/2009 vốn điều lệ của TRUSTBank là 1.500 tỉ đồng (Một nghìn năm trăm tỉ đồng).

II - Sản phẩm dịch vụ chính:

TRUSTBank cung cấp đa dạng các sản phẩm, dịch vụ tài chính phù hợp với nhu cầu của Quý khách hàng như:

- Huy động vốn bằng đồng Việt Nam, ngoại tệ;
- Cung cấp tín dụng, đầu tư, góp vốn liên doanh bằng đồng Việt Nam, ngoại tệ;
- Các dịch vụ thanh toán trong nước, dịch vụ ngân quỹ, chuyển tiền kiều hối & chuyển tiền nhanh, bảo hiểm nhân thọ qua ngân hàng;
- Thanh toán quốc tế & kinh doanh ngoại tệ.



III - Mạng lưới hoạt động: Hiện nay, TRUSTBank gồm **51** chi nhánh và phòng giao dịch tại các tỉnh thành thuộc vùng kinh tế trọng điểm trong cả nước. Dự kiến đến cuối năm 2009, mạng lưới hoạt động của TRUSTBank bao gồm 60 chi nhánh/ phòng giao dịch tại khắp các tỉnh, thành phố, trung tâm kinh tế trên cả nước.

IV - Nhân sự:

Tính đến ngày **23/10/2009** tổng số nhân viên của TRUSTBank là **668** người. Đa số cán bộ nhân viên có trình độ đại học và trên đại học, thường xuyên được đào tạo chuyên môn nghiệp vụ tại trung tâm đào tạo của TRUSTBank và các trường Đại học, Viện nghiên cứu trong nước.

V - Định hướng & Mục tiêu phát triển: TRUSTBank định hướng trở thành một trong những Ngân hàng TMCP đô thị phát triển, có nghiệp vụ đa dạng, chất lượng phục vụ cao, công nghệ ngân hàng hiện đại, mạng lưới kênh phân phối rộng dựa trên nền tảng mô hình tổ chức và quản lý theo chuẩn mực quốc tế, công nghệ thông tin hiện đại, công nghệ ngân hàng tiên tiến, từng bước đưa TRUSTBank trở thành một thương hiệu ngân hàng bán lẻ có uy tín trên thị trường tài chính trong nước và quốc tế.

TRUSTBank sẽ tiếp tục đưa ra các giải pháp mới nhằm đạt được các mục tiêu đã đề ra:

1. **Tăng vốn điều lệ:** lên 3.000 tỷ đồng (đến năm 2010).

2. **Phát triển nguồn vốn huy động:** hiện đại hóa công nghệ ngân hàng trực tuyến, cho ra các sản phẩm đa dạng, chương trình khuyến mại phù hợp, đáp ứng nhu cầu thiết thực và tốt nhất với từng đối tượng khách hàng.

3. **Xác định đối tượng và chính sách hoạt động kinh doanh:** xác định đối tượng đầu tư tín dụng phù hợp; nghiên cứu đầu tư, tham gia liên doanh góp vốn đối với một số dự án trọng điểm; cơ cấu lại tài sản sinh lời nhằm đảm bảo hoạt động an toàn và ổn định.

4. **Xác định thị trường và lĩnh vực kinh doanh khác:** nhanh chóng nắm bắt các cơ hội kinh doanh trên thị trường mục tiêu, có kế hoạch thâm nhập các thị trường tiềm năng.

5. **Phát triển các dịch vụ Ngân hàng:** nâng cấp chất lượng dịch vụ hiện có, tạo điều kiện hỗ trợ cho các nghiệp vụ khác phát triển, liên kết với các Ngân hàng bạn để phát triển các dịch vụ Ngân hàng.

6. **Phát triển mạng lưới hoạt động** nhằm giúp cho Ngân hàng tiếp cận và mang sản phẩm đến với khách hàng.

7. **Phát triển nguồn nhân lực.**

8. **Hiện đại hóa công nghệ Ngân hàng.**

VI - Cam kết: Với mục đích mang đến lợi nhuận tốt nhất cho các cổ đông, song song với việc đáp ứng nhu cầu khách hàng, TRUSTBank cam kết phục vụ một cách hiệu quả cho toàn thể khách hàng cũng như CB-CNV của TRUSTBank, bằng cách:

- Đẩy mạnh cải cách nhằm đạt tới những chuẩn mực, thông lệ quốc tế về hoạt động tiền tệ, ngân hàng, tiếp tục nâng cao năng lực tài chính, chất lượng tín dụng để tiếp cận các tiêu chuẩn quốc tế.
- Hướng đến hiện đại hóa công nghệ ngân hàng để nhanh chóng tiếp cận và phát triển các dịch vụ ngân hàng thương mại hiện đại - đa năng, tăng cường công tác quản lý rủi ro nhằm đáp ứng các tiêu chuẩn quốc tế về hệ số an toàn tín dụng, nâng cao hiệu quả kinh doanh cũng như năng lực cạnh tranh.
- Chú trọng đẩy mạnh công tác huy động vốn với nhiều hình thức phong phú, đáp ứng kịp thời nhu cầu vốn của các thành phần kinh tế trên phạm vi cả nước.
- Nhanh chóng mở rộng mạng lưới hoạt động tại các tỉnh, thành vùng kinh tế trọng điểm trong cả nước.
- Phát triển sản phẩm thẻ (ATM, thẻ tín dụng) nhằm nâng cao chất lượng phục vụ khách hàng.
- Tăng cường quan hệ và thu hút các cổ đông chiến lược là các Ngân hàng hàng đầu trong và ngoài nước, các tập đoàn kinh tế lớn, tiềm lực tài chính mạnh.



- Quan tâm nâng cao chất lượng phục vụ khách hàng, đưa ra các giải pháp chăm sóc hữu hiệu, đáp ứng cao nhất các nhu cầu hợp lý của khách hàng.
- Nghiên cứu phát triển đa dạng hóa các sản phẩm.



8. Secude



GIỚI THIỆU VỀ SECUDE

Giới thiệu chung

SECUDE là nhà cung cấp và phát triển các giải pháp bảo mật thông tin cho doanh nghiệp. Là đối tác chính thức của SAP, Citrix, Microsoft, sản phẩm và dịch vụ tư vấn của chúng tôi cam kết mang lại sự an toàn và hiệu quả cao trong bảo mật thông tin, dữ liệu cho khách hàng là các doanh nghiệp trên khắp thế giới.

SECUDE thành lập vào năm 1996, từ sự cộng tác giữa SAP AG và viện Fraunhofer Institute. Với trụ sở chính đặt tại Thụy Sĩ, chúng tôi phát triển hệ thống đối tác và khách hàng toàn cầu dựa vào mạng lưới các văn phòng, chi nhánh tại Châu Âu, Châu Á và khu vực Trung Đông.

SECUDE Việt Nam chính thức đi vào hoạt động từ 01/02/2007, theo định hướng và chiến lược mở rộng kinh doanh và sản xuất sang khu vực Châu Á của tập đoàn.

SECUDE Việt Nam hiện nay tập trung cho hai bộ phận: R&D (nghiên cứu và phát triển sản phẩm) và bộ phận Tư vấn, Tiếp thị toàn cầu. Đội ngũ SECUDE Việt Nam thường xuyên được tham gia các chương trình đào tạo, huấn luyện tại công ty mẹ ở Châu Âu để nâng cao tay nghề, trình độ, kiến thức về công nghệ. Với quy mô và tốc độ phát triển hiện nay, cộng với hiệu quả công việc đóng góp cho tập đoàn, SECUDE Việt Nam ngày càng khẳng định vị trí và tầm quan trọng của mình đối với SECUDE toàn cầu.

Để tìm hiểu thêm về SECUDE, vui lòng truy cập website: www.secude.com

Tầm nhìn

SECUDE nỗ lực hướng đến các giải pháp an toàn thông tin trong môi trường SAP và IT thông qua việc nghiên cứu, phát triển những công nghệ tiên phong và hướng đến khách hàng.

Sứ mệnh

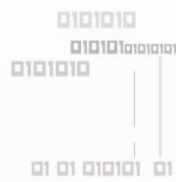
Chủ động phát triển các sản phẩm và giải pháp tư vấn về an toàn thông tin phù hợp và tương ứng cho môi trường SAP và ngoài SAP để bảo vệ hệ thống và mạng lưới của doanh nghiệp trước những nguy cơ hoặc rủi ro trên toàn thế giới.

Trọng tâm đầu tư

SECUDE đầu tư cho công nghệ và nghiên cứu về bảo mật thông tin để mang lại các giải pháp đa dạng, tối ưu cho thị trường toàn cầu.

SECUDE hiện nay đang phát triển 3 nhóm sản phẩm, dịch vụ chính sau đây:

1. Nhóm sản phẩm về bảo mật thông tin trong môi trường IT (dưới thương hiệu FinallySecure)
2. Nhóm sản phẩm về bảo mật thông tin trong môi trường SAP
3. Tư vấn về an toàn, bảo mật thông tin.

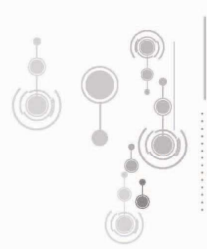


Nhóm sản phẩm bảo mật thông tin trong môi trường IT

- FinallySecure Enterprise
- Secure Device
- Secure SignOn
- Secure TrustManager

Nhóm sản phẩm bảo mật thông tin trong môi trường SAP

- Secure Login
- Secure Doc
- CodeProfiler

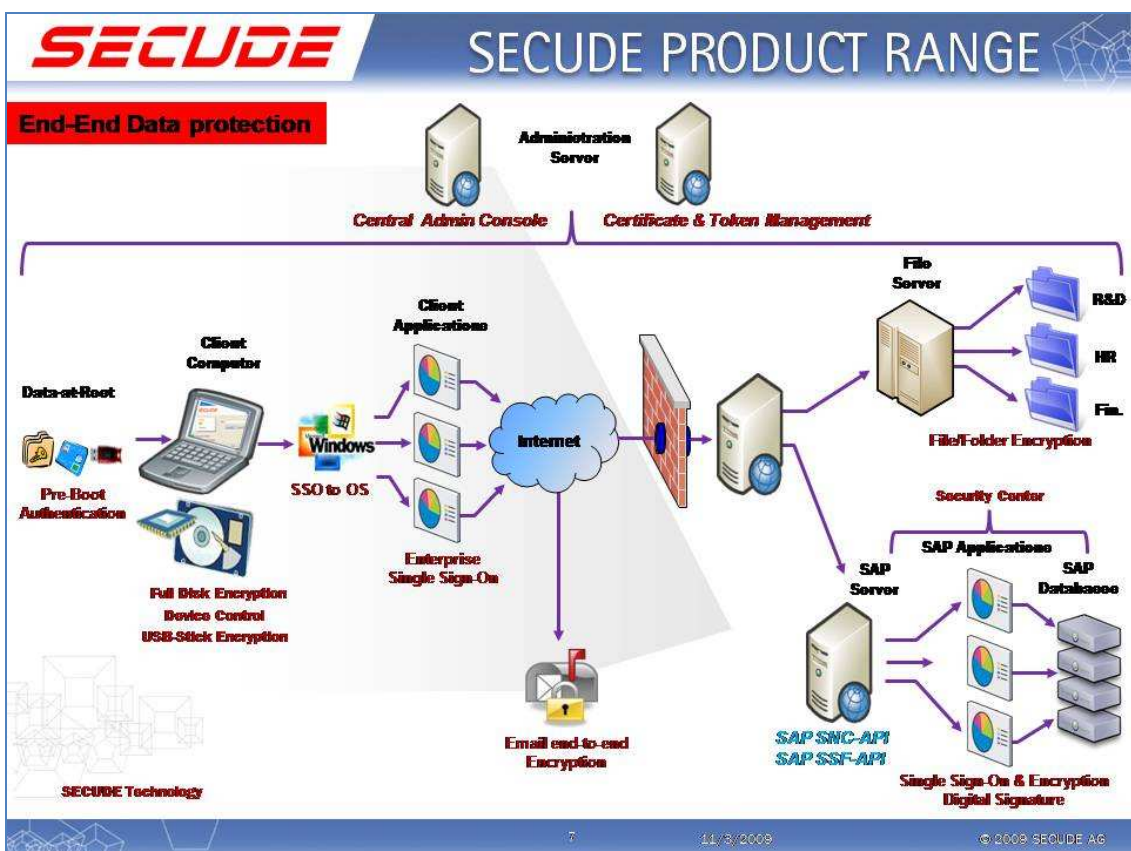
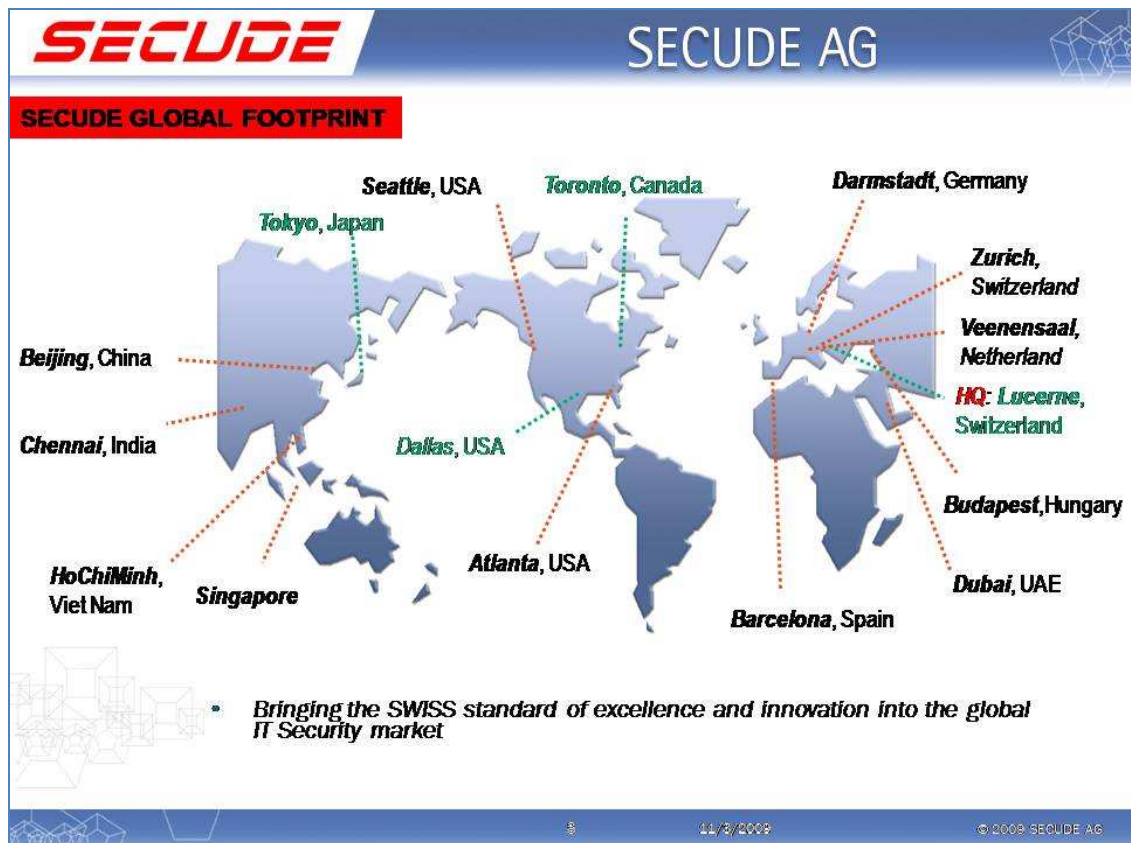


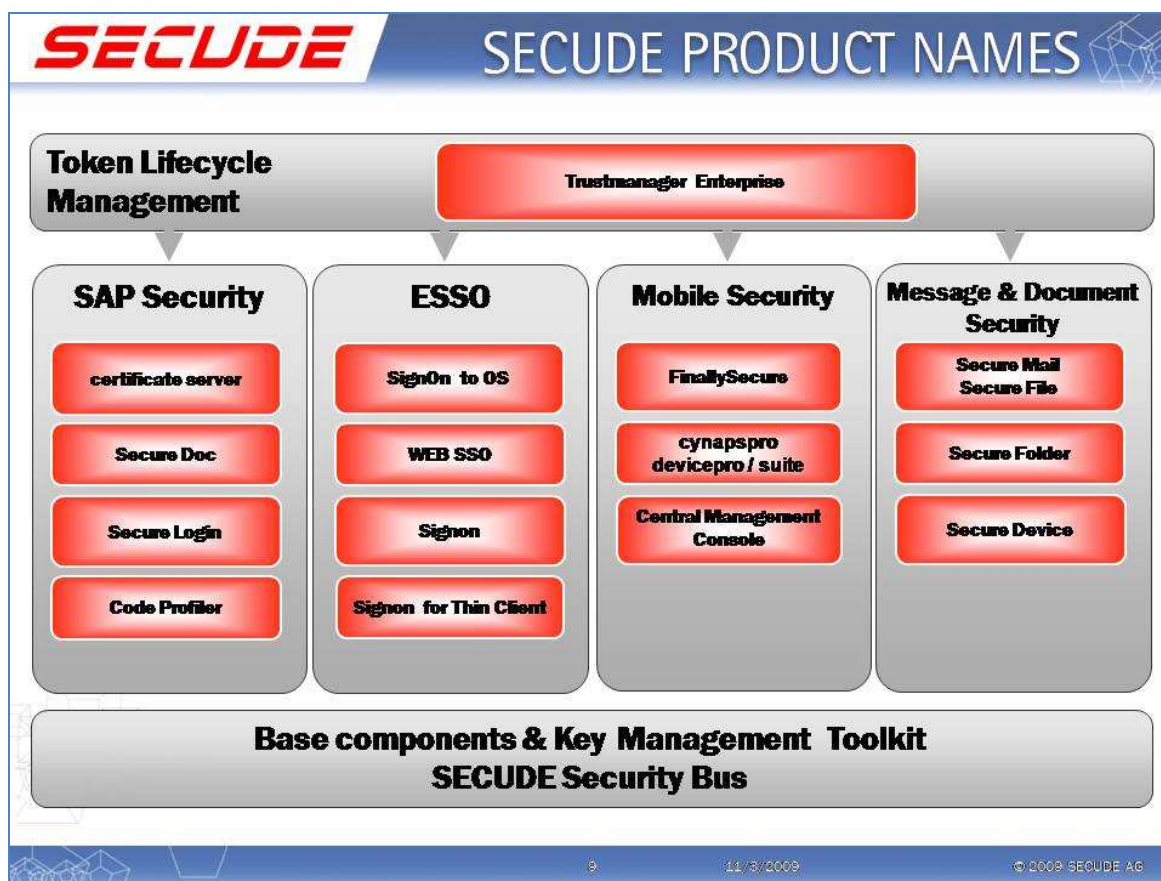
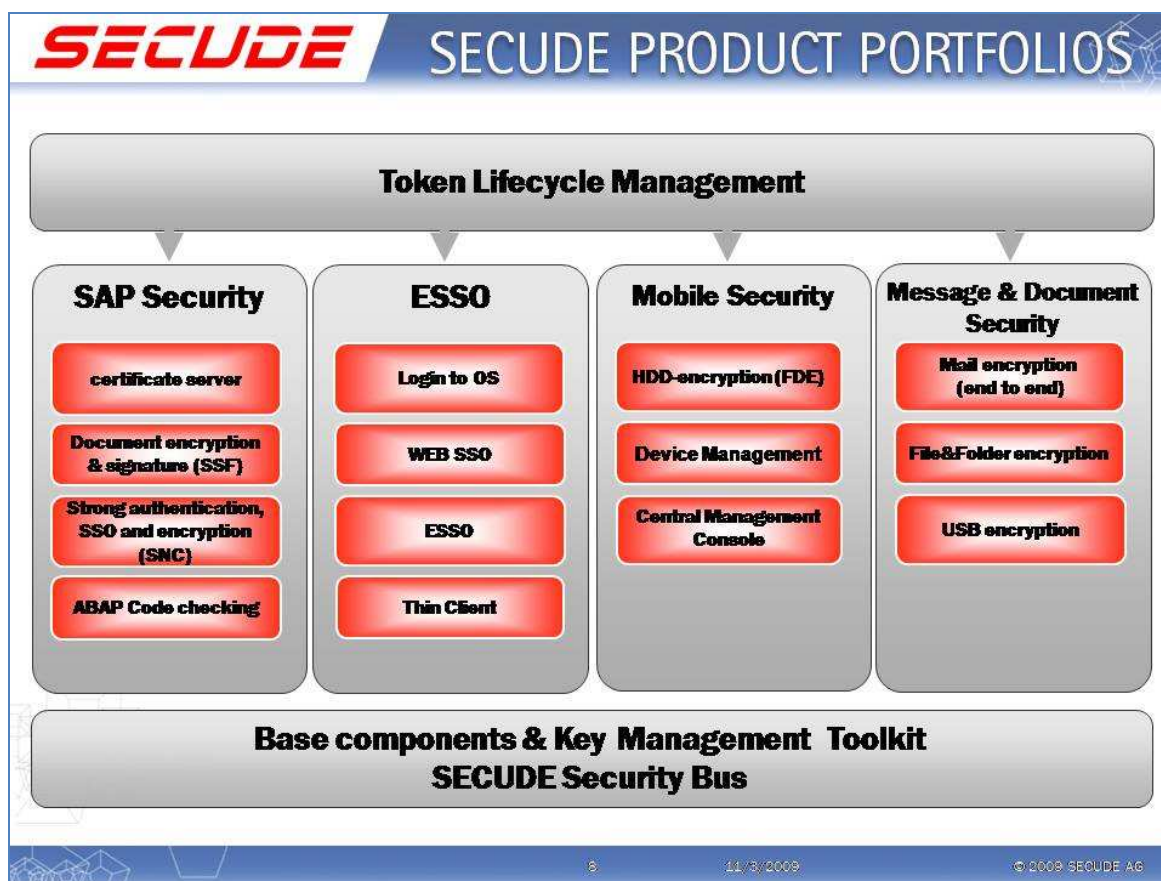
www.secude.com

Công ty TNHH
SECUDE International
44B Phan Xích Long, P.3, Q.PN
TP.HCM/ Việt Nam

ĐT : +84 8 399 56 854
Fax : +84 8 399 56 851
Email: salesvn@secude.com
Website: www.secude.com

©2009 SECUDE AG





9. Kaspersky



www.kaspersky.vn

Giới thiệu sản phẩm Kaspersky:

Kaspersky Lab trở thành thương hiệu số 1 về anti-virus tại Việt Nam. Kaspersky Lab mang đến cho khách hàng sự yên tâm để khách hàng kết nối an toàn vào không gian công nghệ đầy cảm hứng. Chỉ trong vòng 2 năm xuất hiện tại Việt Nam, NTS Group đại diện thương hiệu Kaspersky Lab đã đưa thương hiệu Kaspersky Lab trở thành lựa chọn tốt nhất cho người dùng máy tính & laptop tại Việt Nam và vinh dự nhận được:

- Giải thưởng Phần mềm diệt virus tốt nhất Việt Nam hai năm liền (năm 2008 & năm 2009) do các Giám đốc Điều hành và Giám đốc CNTT bầu chọn và Tập đoàn Dữ liệu Quốc tế (IDG) tổ chức.
- Giải thưởng Sản phẩm CNTT-TT ưa chuộng nhất năm 2009 do độc giả Tạp chí PC World Việt Nam bầu chọn.
- Chứng nhận Vàng về Anti-Rootkit của Phòng thí nghiệm ATTT trọng điểm quốc gia.

Sản phẩm Kaspersky Lab bao gồm:

- Sản phẩm Kaspersky dành cho cá nhân (KIS/KAV/KMS)
- Sản phẩm Kaspersky dành cho doanh nghiệp (Kaspersky Open Space Security (KOSS))

10. Astaro



Astaro dẫn đầu công nghệ tường lửa trên nền Linux (Firewall). Các dòng sản phẩm đa dạng của Astaro tích hợp 10 lớp bảo vệ chống lại các nguy cơ ăn cắp dữ liệu, virus tấn công, virus gián điệp, spam. Các dòng sản phẩm Astaro ngày càng được ưa chuộng tại Việt Nam: Astaro Security Gateway, Astaro Web Gateway, Astaro Mail Gateway, Astaro Command Center, Astaro Report Manager, Astaro VPN Clients, Astaro Compliance Reporter. Tập đoàn nghiên cứu dữ liệu thị trường hàng đầu GFK Group đã chọn lựa Astaro để bảo vệ dữ liệu thông tin vô giá của các khách hàng của họ trên toàn cầu. Astaro đang trở thành thương hiệu có ảnh hưởng lớn đến sự phát triển của công nghệ firewall dành cho các doanh nghiệp trên toàn thế giới.

- Astaro Security Gateway 110/120
- Astaro Security Gateway 220
- Astaro Security Gateway 320
- Astaro Security Gateway 425
- Astaro Security Gateway 525/525F

11. Khu CNPM Đại học quốc gia TP.HCM

Tên tổ chức: **Khu Công nghệ Phần mềm Đại học quốc gia Thành phố Hồ chí Minh.**

Tên tiếng Anh: **Information Technology Park – Vietnam National University at Ho Chi Minh city.**

Viết tắt: **VNU-ITP**

Địa chỉ: **Khu phố 6, phường Linh trung, Quận Thủ đức, TpHCM**

<http://www.vnu-ity.edu.vn>

VNU-ITP là một tổ chức công lập hoạt động trong lĩnh vực phát triển khoa học công nghệ của Đại học quốc gia TpHCM. Khu CNPM ĐHQG-HCM có nhiệm vụ xây dựng môi trường công nghiệp trong đại học nhằm nâng cao chất lượng đào tạo và nghiên cứu khoa học của ĐHQG-HCM.

PHẦN 3: THÔNG TIN ĐƠN VỊ TỔ CHỨC VÀ HỘI VIÊN

1. SỞ THÔNG TIN VÀ TRUYỀN THÔNG TP. HỒ CHÍ MINH

Sở Thông tin và Truyền thông thành phố Hồ Chí Minh là cơ quan quản lý nhà nước tại địa phương, có chức năng tham mưu, giúp Ủy ban nhân dân thành phố thực hiện chức năng quản lý nhà nước về các lĩnh vực:



- Báo chí, xuất bản
- Bưu chính - Viễn thông
- Công nghệ thông tin
- Điện tử
- Internet
- Truyền dẫn phát sóng
- Tần số vô tuyến điện
- Phát thanh, truyền hình
- Cơ sở hạ tầng thông tin
- Quảng cáo trên các phương tiện báo chí, mạng thông tin máy tính và xuất bản phẩm.
- Quản lý các dịch vụ công về bưu chính, viễn thông và công nghệ thông tin trên địa bàn thành phố.

Ngoài ra Sở Thông tin và Truyền thông còn thực hiện một số nhiệm vụ, quyền hạn theo sự ủy quyền của Ủy ban nhân dân thành phố Hồ Chí Minh và đồng thời chịu sự chỉ đạo, kiểm tra về nghiệp vụ chuyên môn của Bộ Thông tin và Truyền thông theo quy định của pháp luật.

Được thành lập và đi vào hoạt động từ tháng 12 năm 2004 với tên gọi Sở Bưu chính, Viễn thông, ngày 13/06/2008, Sở Bưu chính, Viễn thông chính thức được đổi tên là Sở Thông tin và Truyền thông, ngoài những chức năng đã được Ủy ban nhân dân thành phố giao trước đây, Sở Thông tin và Truyền thông còn được bổ sung thêm chức năng quản lý về báo chí, xuất bản và phát thanh, truyền hình theo quyết định số 49/2008/QĐ- UBND của Ủy ban nhân dân thành phố Hồ Chí Minh.

Tiếp tục phát huy những kết quả đạt được của giai đoạn trước đây về triển khai xây dựng chính phủ điện tử tại thành phố, tạo bước đột phá trong ứng dụng CNTT góp phần đưa TP. HCM trở thành địa phương dẫn đầu cả nước về ứng dụng CNTT – TT trong quản lý nhà nước; đẩy mạnh các hoạt động trong quản lý hạ tầng Viễn thông – Internet, góp phần đưa chỉ số sẵn sàng CNTT – TT của TP. HCM lên vị trí hàng đầu của cả nước. Sở Thông tin và Truyền thông đã chuẩn bị sẵn sàng những chương trình, kế hoạch hành động tiếp theo nhằm đáp ứng được nhiệm vụ mới được giao trong giai đoạn tới.

Thông tin liên hệ:

Trụ sở: 59 Lý Tự Trọng, Quận 1, Tp. Hồ Chí Minh

Điện thoại: (84 – 8) 3 520 2727

Website: www.ict-hcm.gov.vn

Fax: (84 – 8) 3 520 2424

Email: sttt@tphcm.gov.vn

2. HIỆP HỘI ATTT VIỆT NAM và CHI HỘI ATTT PHÍA NAM



Hiệp hội ATTT Việt Nam (VNISA), thành lập vào tháng 7/2007, là tổ chức xã hội nghề nghiệp tự nguyện phi lợi nhuận đầu tiên hoạt động trong lĩnh vực bảo mật được Nhà Nước công nhận. VNISA tập hợp các cá nhân, tổ chức làm công tác nghiên cứu, giảng dạy, ứng dụng và phát triển ATTT; những người có quan tâm, có đóng góp, tạo điều kiện cho sự nghiệp khoa học công nghệ và phát triển các ứng dụng trong lĩnh vực ATTT theo nhu cầu cuộc sống và định hướng chiến lược về ATTT của Nhà Nước Việt Nam.

lược về ATTT của Nhà Nước Việt Nam.

Chi nhánh phía Nam của Hiệp Hội là chi hội ATTT Phía Nam, đã ra mắt vào tháng 9/2008, với ban điều hành lâm thời gồm 12 người do ông Ngô Vi Đồng - tổng giám đốc HPT, phó chủ tịch hiệp hội VNISA làm chủ tịch Chi Hội. Hiện tại Chi Hội đã có 10 hội viên (55 cá nhân và 45 tập thể-đơn vị) đã tự nguyện tham gia.

Chi hội phía Nam sẽ tiếp tục thực hiện tôn chỉ, mục đích của VNISA, đồng thời khẳng định tầm quan trọng của vấn đề ATTT trong mọi hoạt động của tổ chức, nhằm giảm thiểu thiệt hại và gia tăng lợi nhuận, hiệu quả công việc cũng như các cơ hội kinh doanh, tạo ra giá trị gia tăng trên từng sản phẩm dịch vụ.

Chi hội phía Nam đã đưa ra quy chế hội viên gồm 5 điều, trong đó ghi rõ: hội viên và điều kiện để trở thành hội viên; các loại hình hội viên; quyền lợi - nghĩa vụ và các điều khoản thi hành.

Thông tin liên hệ:

Văn phòng của Chi hội: 60 Nguyễn Văn Trỗi, Q.Phú Nhuận, TP.HCM

Điện thoại: (84 – 8) 3 845 8518 (ext: 1311) Fax: (84 – 8) 3 845 8516

Liên hệ: Huỳnh Ngọc Hân. Email: hanhn@vnisa.org

Chi Hội VNISA phía Nam qua các sự kiện

Thành lập Chi hội ATTT (ATTT) phía nam:

Ngày 20/9/2008, tại TP.HCM, hiệp hội ATTT Việt Nam (VNISA) đã ra mắt chi hội ATTT phía Nam do ông Ngô Vi Đồng – Tổng giám đốc công ty cổ phần Dịch Vụ Công Nghệ Tin Học HPT, Phó Chủ tịch Hiệp hội ATTT Việt Nam làm Chủ tịch cùng với 11 ủy viên ban điều hành.

Ban đầu, Chi hội được thành lập với 76 hội viên, trong đó có 47 hội viên tập thể là các doanh nghiệp và 29 hội viên cá nhân.

Điểm qua một số công tác của Chi hội trong năm 2008:

- o Ngày 13 tháng 8 năm 2008, Chi hội thành lập Ban Chấp Hành lâm thời gồm 12 thành viên, và ban thư ký. Ông Ngô Vi Đồng giữ chức vụ Chủ tịch Chi hội cùng 11 ủy viên Ban chấp hành và ông Trần Anh Minh giữ chức vụ Tổng Thư ký Chi hội.

Thành lập 6 ban chuyên môn và có các trưởng ban chuyên trách.

- o Ngày 23/08/2008, tại Khách sạn Palace, Chi hội phối hợp với Báo Doanh nhân Sài Gòn tổ chức hội thảo “Quảng bá hiệu quả và an toàn thương mại qua website”.
- o Tháng 10 năm 2008, Chi hội kết hợp với VCCI tổ chức hội thảo “Nâng cao nhận thức về ATTT cho doanh nghiệp vừa và nhỏ”.

Ngoài ra, Chi hội đã tổ chức thực hiện khảo sát thực trạng ATTT của các tổ chức và doanh nghiệp.

- o Ngày 18/11/2008, Chi hội tổ chức thành công ngày ATTT Việt Nam tại TP. HCM với chủ đề “ATTT là bảo vệ tài sản doanh nghiệp” với hơn 300 khách mời gồm Doanh nghiệp, Sở Ban ngành TP, và cơ quan Báo chí Truyền thông.

Báo cáo chuyên đề của Ngày ATTT năm 2008 tập trung vào 3 mảng lớn với các đề tài: An toàn mạng thông tin doanh nghiệp (do đại diện ZyXEL, Oak Well, Data Terminator, Misoft và trung tâm Quản Lý Tàn Số 2 trình bày); đào tạo và chuẩn hóa ATTT (do ĐH KHTN TP.HCM và Athena trình bày); an ninh thương mại điện tử (do Microsoft, Kaspersky và Ngân hàng Việt Á trình bày).

Ngày ATTT lần thứ nhất đã đạt được mục tiêu đề ra là tạo ra một diễn đàn chung cho các tổ chức, doanh nghiệp, các chuyên gia trong lĩnh vực ATTT của khu vực phía Nam cũng như trên cả nước và quốc tế. Tại đây, các bên tham gia có dịp tiếp xúc với đại diện các cơ quan quản lý nhà nước liên quan để chia sẻ nhận thức, trách nhiệm, kinh nghiệm trong việc quản lý chính sách cũng như các giải pháp cụ thể nhằm tạo điều kiện thuận lợi cho việc nâng cao nhận thức và phát triển ứng dụng ATTT tại thành phố Hồ Chí Minh.

Hoạt động của Chi hội trong năm 2009:

Sau Ngày ATTT lần thứ nhất năm 2008, Chi hội tiếp tục hoạt động mạnh mẽ và có những thành công rõ nét trong năm 2009. Đến nay, Chi hội đã phát triển được 10 hội viên, trong đó có 45 Hội viên đơn vị và 55 hội viên cá nhân. Chi hội thường xuyên tổ chức gặp gỡ, giao lưu giữa các hội viên nhằm tạo môi trường sinh hoạt vui vẻ, thân thiện, hiểu biết lẫn nhau; hợp tác và giao lưu với các hội bạn.

Sau đây là một số hoạt động chính của Chi hội từ đầu năm 2009 đến nay:

- o Ngày 27/3/2009, tại TP.HCM, Chi hội đã họp mặt đầu năm và triển khai kế hoạch năm 2009 với mục đích hoạt động theo hướng phục vụ phát triển ngành nghề ATTT, hỗ trợ các hội viên trong lĩnh vực ATTT và cùng các hội viên vượt qua khó khăn trong cuộc suy thoái kinh tế toàn cầu.

Cũng trong ngày này, Chi hội đã tổ chức báo cáo chuyên đề “Web 2.0 Security: Xu hướng và hiểm họa”.

- o Ngày 15/4/2009, Chi hội ký kết “Thỏa thuận hợp tác” với Hiệp hội Thương Mại Điện Tử Việt Nam (VECOM).
- o Ngày 17/4/2009, Chi hội đã phối hợp với Sở Thông tin & Truyền thông tổ chức hội thảo chuyên đề “ATTT cho các hệ thống công nghệ thông tin TP.HCM”. Trong hội thảo, Sở và Chi hội đã báo cáo hiện trạng triển khai ATTT, đề xuất mô hình quản lý ATTT và các dịch vụ ứng cứu.
- o Tháng 5/2009, Chi hội xây dựng Quy chế hình thành tổ chức tình nguyện viên tình nguyện trong các hội viên của mình bao gồm các chuyên gia giỏi về ATTT có kỹ thuật và đạo đức nghề nghiệp để cùng chia sẻ kinh nghiệm và sẵn sàng tham gia vào các hoạt động tư vấn, ứng cứu khẩn cấp cho các cơ quan, doanh nghiệp khi có yêu cầu. Tổ chức được gọi tên “Vnisa Elite Team”.
- o Ngày 11/6/2009, tại văn phòng Chi hội, Elite Team đã họp mặt chia sẻ về nhiệm vụ đầu tiên là đánh giá ATTT cho Sở Thông tin và Truyền thông TP.HCM.
- o Ngày 19/6/2009, Chi hội tổ chức thành công hội thảo “Ảo hóa an ninh – Giải pháp thời suy thoái” tại TP.HCM.
- o Ngày 30/6/2009, Chi hội và Tạp chí Thế giới vi tính (PCW) phối hợp tổ chức buổi hội thảo – tọa đàm chuyên đề “ATTT trong hoạt động truyền thông” tại Tòa soạn Tạp chí PCW.
- o Ngày 29/7/2009, tại TP.HCM, Chi hội và Báo Doanh nhân Sài Gòn đã tổ chức hội thảo “An ninh nội bộ - Chính sách An toàn thông tin”.
- o Ngày 17/8/2009, các thành viên Ban Chấp hành Chi hội đã có buổi tiếp đoàn Viện phát triển xã hội thông tin Hàn Quốc (KISDI). Trong buổi làm việc, đoàn KISDI muốn tìm hiểu về hiện trạng ATTT ở Việt Nam cũng như những khó khăn đang gặp phải và vai trò của chính phủ trong hiện trạng ATTT Việt Nam.
- o Ngày 25/8/2009, tại TP.HCM, Chi hội cùng Entrust, HP, Ngân hàng Việt Á, và Payoo tổ chức hội thảo “ATTT trong thương mại điện tử”.
- o Từ ngày 14/9 – 16/9/2009, Chi hội kết hợp với công ty Vietshield và công ty HPT tổ chức thành công khóa học Foundstone Ultimate Hacking dành cho các hội viên và doanh nghiệp quan tâm đến vấn đề đảm bảo ATTT cho môi trường Web.
- o Ngày 19/9/2009, tại TP. HCM, Chi hội phối hợp với Sở Thông tin & Truyền thông và Công ty Tư vấn Trắng Xanh đã tổ chức hội thảo “ATTT trong phần mềm ứng dụng” xoay quanh các chủ đề: Tầm quan trọng của an ninh ứng dụng, bẻ khóa phần mềm, phương pháp và cách phòng chống, các kỹ thuật gian lận trong trò chơi trực tuyến.

Và hoạt động quan trọng nhất trong năm vẫn là công tác tổ chức ngày ATTT. Sau thành công của “Ngày ATTT Việt Nam” lần thứ nhất được tổ chức vào ngày 18/11/2008, Sở Thông tin & Truyền thông TP.HCM và Chi hội tiếp tục phối hợp tổ chức “Ngày ATTT Việt Nam” lần thứ hai với chủ đề “Bảo vệ tài nguyên thông tin hôm nay, vì ngày mai phát triển”. Sự kiện sẽ diễn ra vào ngày 18/11/2009 tại khách sạn New World, TP.HCM.

“Ngày ATTT Việt Nam 2009” tại TP.HCM nằm trong khuôn khổ các sự kiện thường niên quy mô quốc gia của Hiệp hội VNISA, cùng dựa trên những mục tiêu chung của Hiệp hội và thể hiện sự gắn kết giữa Nhà nước – Xã hội – Doanh nghiệp, và cũng là cơ hội tiếp cận, chia sẻ những kiến thức, công nghệ bảo mật tiên tiến nhất trong lĩnh vực ATTT.

3. HPT



CÔNG TY CỔ PHẦN DỊCH VỤ CÔNG NGHỆ TIN HỌC HPT

Địa chỉ: 60 Nguyễn Văn Trỗi, Q. Phú Nhuận, Tp.HCM.

Điện thoại: 08 3845 8518 - Fax: 08 3845 8516

Web site : www.hpt.vn - Email : info@hpt.vn

Mục tiêu hoạt động

“Thấu hiểu và phát triển những ứng dụng công nghệ tiên tiến trong lĩnh vực CNTT và Truyền thông cho khách hàng tại Việt Nam và quốc tế vì sự phồn vinh của khách hàng, của HPT và của Việt Nam”

“HPT mong muốn trở thành một tổ chức văn minh hiện đại có năng lực phát triển mạnh mẽ, thành công và thịnh vượng, là niềm tự hào của tri thức Việt Nam trong công cuộc hội nhập toàn cầu hoá, là môi trường cho nhân tài phát triển, xứng đáng là một trong những trụ cột kinh tế kỹ thuật của Việt Nam”

Nguồn nhân lực

Đội ngũ quản lý điều hành

HPT xây dựng đội ngũ cán bộ điều hành tài giỏi, có bản lĩnh

Đội ngũ chuyên gia

HPT có đội ngũ chuyên gia với nhiều năm kinh nghiệm thực tiễn trong các lĩnh vực sau:

- Xây dựng hạ tầng cơ sở CNTT và tích hợp hệ thống
- Bảo mật và an toàn thông tin
- Tư vấn triển khai và ứng dụng CNTT
- Phát triển phần mềm, cung cấp dịch vụ phần mềm
- Thực hiện sửa chữa, bảo hành, bảo trì hệ thống CNTT
- Tư vấn đào tạo nguồn nhân lực CNTT và các kỹ năng mềm
- Kỹ năng quản trị tài chính và kiểm soát chất lượng

Hạ tầng CNTT

Các ứng dụng và chính sách ATTT

Hạ tầng CNTT hiện đại, an toàn và thông suốt

Các hệ thống mạng nội bộ, đường truyền, hệ thống máy chủ, hệ thống CoreIO... được trang bị hiện đại, đảm bảo hoạt động xuyên suốt, phục vụ cho việc lưu trữ, chia sẻ và tối ưu hoá tài nguyên dùng chung.

Ứng dụng CNTT phục vụ cho quản trị và kinh doanh

Hệ thống quản lý tổng thể doanh nghiệp ERP Oracle e-Business Suite, chương trình quản lý nguồn nhân lực HPT- HRM được triển khai ứng dụng trong toàn công ty

Hệ thống CNTT đáp ứng các tiêu chuẩn về An toàn thông tin (ATTT)

HPT xây dựng các chính sách về an toàn CNTT và áp dụng toàn công ty. Việc bảo mật được triển khai ở nhiều mức khác nhau

Hệ thống chất lượng

Chính sách chất lượng:

HPT áp dụng Chính sách Chất lượng theo tiêu chuẩn ISO 9001:2000 cho các hoạt động dịch vụ phục vụ khách hàng và cho các quy trình quản lý của Công ty.

- Trong sản xuất phần mềm HPT đạt chuẩn CMMi Level 3
- Trong An toàn Thông tin HPT hướng đến đạt chuẩn ISO27001
- Cam kết của Lãnh đạo về chất lượng dịch vụ và sản phẩm

Lĩnh vực hoạt động

1. Tích hợp hệ thống

- Cung cấp các giải pháp hạ tầng, Data center đảm bảo thiết kế chuẩn quốc TIA, ISO...
- Cung cấp giải pháp hệ thống máy chủ và lưu trữ cho doanh nghiệp
- Cung cấp giải pháp mạng và truyền thông hợp nhất
- Cung cấp giải pháp bảo mật
- Giải pháp dịch vụ cơ sở dữ liệu
- Dịch vụ:
 - Dịch vụ triển khai, hỗ trợ kỹ thuật
 - Dịch vụ triển khai trên diện rộng
 - Dịch vụ bảo trì và hỗ trợ kỹ thuật cho các hệ thống quan trọng
 - Dịch vụ di dời, tái cấu trúc hệ thống...

2. Dịch vụ phần mềm và Phát triển phần mềm

Dịch vụ Phần mềm:

Cung cấp dịch vụ triển khai các giải pháp phần mềm của các hãng CNTT hàng đầu thế giới gồm:

- Giải pháp quản lý và hoạch định nguồn lực ERP Oracle
- Giải pháp hệ thống, SharePoint Portal, Dynamics trên nền công nghệ giải pháp Microsoft
- Cung cấp các giải pháp phần mềm hệ thống cao cấp ...

Phát triển phần mềm và outsourcing

Cung cấp phần mềm đóng gói:

- Phần mềm quản lý nguồn nhân lực HPT- HRM
- Phần mềm quản lý hàng khuyến mãi GEM...

Gia công xuất khẩu phần mềm:

- Phát triển các ứng dụng nhúng
- Phát triển phần mềm theo yêu cầu của khách hàng...

3. Dịch vụ bảo hành, bảo trì

- Bảo hành các sản phẩm do HPT cung cấp; Là đại lý ủy quyền của các hãng máy tính lớn
- Cung cấp các dịch vụ bảo trì, hỗ trợ kỹ thuật

Khách hàng

Phạm vi khách hàng

- Cơ quan quản lý nhà nước, Năng lượng dầu khí, Truyền thông báo chí, Thương mại dịch vụ
- Tài chính, Ngân hàng, Bảo hiểm, Viễn thông
- Giáo dục đào tạo, Vận tải, Dược phẩm y tế và Lĩnh vực sản xuất
- Các cơ quan chính phủ, các công ty, tập đoàn đa quốc gia
- Các khách hàng ngoài lãnh thổ Việt Nam

Cam kết với khách hàng

- Đem đến cho khách hàng những giải pháp khả thi, công nghệ phù hợp, tối ưu và tiên tiến
- Đầu tư về công nghệ và nguồn lực phục vụ lâu dài cho khách hàng
- Thực hiện đúng và trọn vẹn những cam kết với khách hàng
- Giữ gìn bảo mật và an toàn hệ thống cho khách hàng
- Chân thành tận tụy với khách hàng
- Cùng với khách hàng thành công “Win-Win” !

Đối tác quốc tế

Đối tác chiến lược của các hãng CNTT hàng đầu Thế giới



Thành tích và khen thưởng

Đối với chính phủ, cơ quan Nhà nước:

- 5 năm liên tiếp đạt bằng khen DN có thành tựu xuất sắc trong lĩnh vực CNTT (UBND TP.HCM)
- 5 Công ty CNTT hàng đầu Việt Nam (HCA)
- Huy chương vàng đơn vị Tích hợp hệ thống CNTT (HCA)
- Doanh nhân Sài Gòn tiêu biểu

Đối với các hãng:

- Nhà cung cấp dịch vụ, giải pháp tốt nhất
- Đối tác cung cấp giải pháp bảo mật tốt nhất
- Nhà cung cấp dịch vụ hỗ trợ kỹ thuật tốt nhất

4. Misoft

MISOFT JSC

Hanoi Office

11 Phan Huy Chu Str., Hanoi, Vietnam

Tel. : (84-4) 3933 1613

Fax : (84-4) 3933 1612

Email : sales@misoft.com.vn

Website: www.misoft.com.vn



Ho Chi Minh City Office

240/2 Pasteur Str., Ward 6, District 3, Ho Chi Minh City, Vietnam

Tel : (84-8) 3820 1018

Fax : (84-8) 3820 0961

Email : misofthcm@misoft.com.vn

Công ty Cổ phần Phát triển Phần mềm và Hỗ trợ công nghệ (Misoft) là công ty đi tiên phong và đứng đầu trong lĩnh vực ATTT tại Việt Nam. Là đối tác chính và là nhà phân phối được ủy quyền của nhiều công ty an ninh mạng hàng đầu thế giới như Check Point, Trend Micro, IBM Internet Security Systems, Crossbeam, Websense, Entrust, Imperva, e-Cop, Passlogix, Vasco, PineApp, Cyber-Ark... công ty Misoft chuyên cung cấp các dịch vụ tư vấn, đào tạo về ATTT, phân phối sản phẩm (phần cứng và phần mềm) an toàn an ninh mạng, triển khai và bảo trì, hỗ trợ kỹ thuật các hệ thống ATTT. Thành lập tháng 5 năm 2001, Misoft luôn duy trì tốc độ tăng trưởng nhanh và bền vững, và được biết đến như là nhà tư vấn và cung cấp giải pháp an ninh mạng chuyên nghiệp hàng đầu Việt Nam với đội ngũ cán bộ, kỹ sư giàu kinh nghiệm trong tư vấn thiết kế, triển khai và hỗ trợ kỹ thuật giải pháp an ninh mạng cho các hệ thống mạng lớn, phức tạp, đặc biệt là trong các lĩnh vực như tài chính - ngân hàng, viễn thông.

Software Development and Technology Promotion Joint Stock Company (Misoft) is the Vietnam's leading in Information Security. Misoft is partner and Authorized Distributor of the global leader in information security as Check Point, Trend Micro, IBM Internet Security Systems, Crossbeam, Websense, Entrust, Imperva, e-Cop, Passlogix, Vasco, PineApp, Cyber-Ark... specializes in providing consulting services, training services for Information Security, providing network security products (hardware and software), implementing and supporting network security systems. Since its inception in May 2001, Misoft has been recognized as a fast and strong growth ICT company in Vietnam. Misoft is known as a company that delivers professional services with extensive experiences in designing, implementing and supporting security solutions of large network, specializes in both Finance - Banking and Telco markets.

CÁC ĐỐI TÁC



CÁC KHÁCH HÀNG TIÊU BIỂU



5. Athena



1, Lịch sử hình thành:

Trung Tâm Đào Tạo Quản Trị & An Ninh Mạng ATHENA được chính thức thành lập theo giấy phép kinh doanh số 410 202 5253 của Sở Kế Hoạch Đầu Tư TP. HCM cấp ngày 04 tháng 10 năm 2004.

ATHENA là một tổ chức quy tụ nhiều trí thức trẻ Việt Nam đầy năng động, nhiệt huyết và kinh nghiệm trong lĩnh vực CNTT. Với tâm huyết góp phần vào công cuộc thúc đẩy tiến trình tin học hóa của nước nhà. ATHENA đã và đang tập trung chủ yếu vào hoạt động như sau:

- Công tác huấn luyện, quảng bá kiến thức tin học đặc biệt trong lĩnh vực mạng máy tính, internet và bảo mật, thương mại điện tử.
- Tư vấn và hỗ trợ cho doanh nghiệp ứng dụng hiệu quả tin học vào hoạt động sản xuất kinh doanh.
- Cung cấp nguồn nhân lực trong lĩnh vực công nghệ thông tin, đặc biệt là các chuyên gia về Mạng Máy Tính và Bảo Mật Mạng đạt trình độ quốc tế cho các tổ chức, doanh nghiệp có nhu cầu.
- Tiến hành các hoạt động nghiên cứu nâng cao kiến thức tin học và phát triển cơ sở dữ liệu thông tin về các ứng dụng và sự cố mạng.
- Tiến hành các dịch vụ ứng cứu khẩn cấp cho doanh nghiệp trong trường hợp xảy ra các sự cố máy tính.
- Tìm kiếm, xác định nguồn gốc mất thông tin, nguồn gốc xâm nhập trái phép vào các hệ thống mạng máy tính doanh nghiệp.
- Kiểm tra định kỳ, hoặc bất kỳ tính an toàn hệ thống thông tin doanh nghiệp
- **Dịch Vụ Cung Cấp & Cho Thuê Nhân Sự IT Doanh Nghiệp**

Đã thành công qua nhiều dự án an ninh mạng cho các công ty lớn , trung tâm An Ninh Mạng Athena đã khẳng định được khả năng và chất lượng dịch vụ an ninh mạng của mình. Nhằm đáp ứng nhu cầu về nhân sự IT từ các doanh nghiệp, trung tâm Athena còn cung cấp dịch vụ cho thuê nhân sự IT

Đội ngũ các nhân viên này được đào tạo kỹ năng thực hành mạng máy tính và Bảo mật mạng đạt trình độ cao . Khi doanh nghiệp có nhu cầu, nhân sự IT do Athena quản lý này sẽ được bố trí làm việc tại các doanh nghiệp như một nhân viên quản trị mạng chính thức trong doanh nghiệp.

2, Đội ngũ nhân viên:

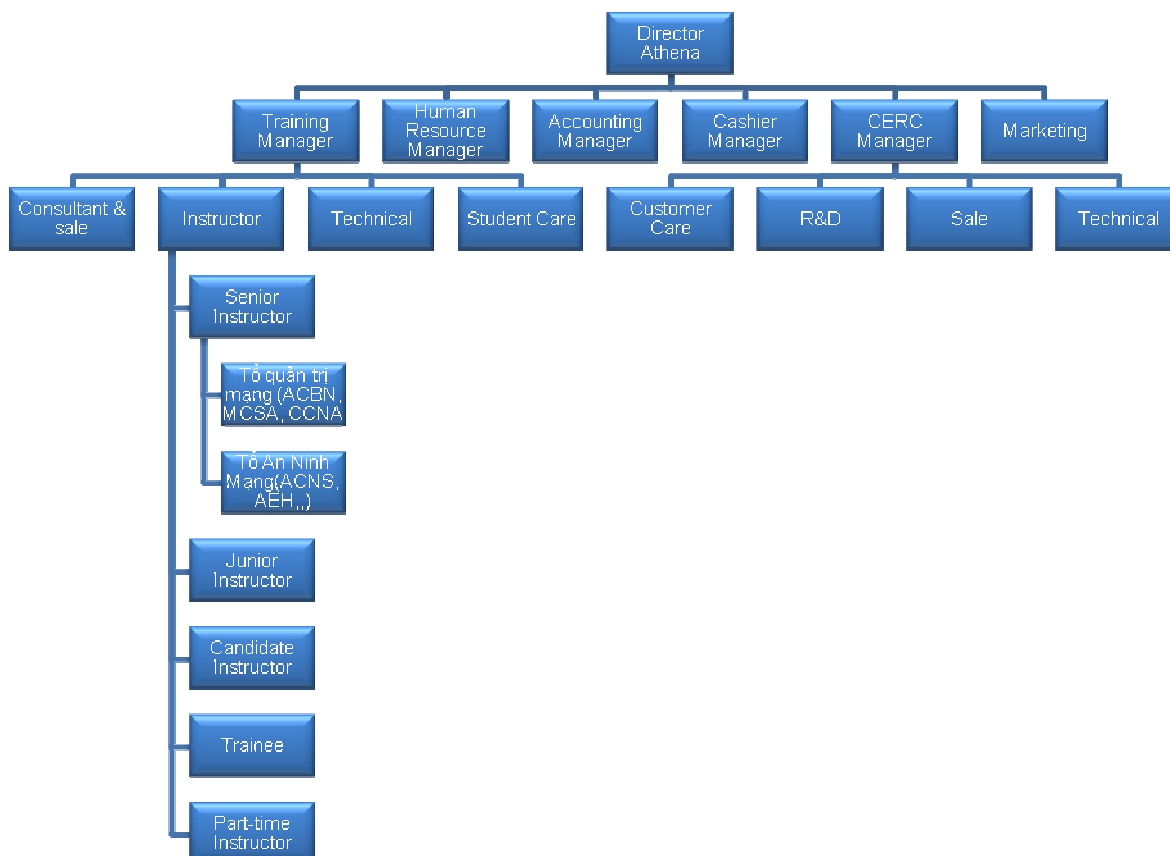
ATHENA không ngừng đầu tư xây dựng đội ngũ, phát triển cơ sở vật chất nhằm mục đích nâng cao chất lượng đào tạo, cung ứng dịch vụ nhằm đáp ứng nhu cầu phát triển kinh tế - xã hội và sự nghiệp công nghiệp hóa - hiện đại hóa đất nước.

Bên cạnh lực lượng hành chánh, kinh doanh và hỗ trợ là lực lượng kỹ thuật và giảng viên tin học, ATHENA hiện đã quy tụ được các chuyên gia xuất sắc trong lĩnh vực CNTT, tốt nghiệp từ các trường Cao Đẳng, Đại Học, Cao Học chuyên ngành CNTT, Điện Tử, Viễn Thông, có nhiều kinh nghiệm làm dự án thực tế và có đầy đủ các chứng chỉ quốc tế

Một số chứng chỉ quốc tế tiêu biểu của nhân viên Athena:

- MCSA, MCSE, MCDBA, MCSD
- Sun Certified Java Programmer/ Developer
- A +, Network +, Security +, Linux+
- Websphere Certification Lotus Note, Domino Server
- HTML/ JavaScript, Web server
- CCNA, CCNP, CCIE
- e-Business Professional, e-Business Consultant CEH

3, Sơ đồ cơ cấu tổ chức trung tâm Athena:



Địa chỉ Athena:

Tên trung tâm: **Trung Tâm Đào Tạo Quản Trị & An Ninh Mạng ATHENA**

Địa chỉ: **2 Bis Đinh Tiên Hoàng, P Đa Kao, Q1, Tp.HCM**

Điện thoại: **1900 54 54 56 – 08.3824 4041**

Email: training@athenavn.com

Website: <http://www.athena.edu.vn>

Cơ sở 2: **Athena-Bách Khoa, Đại Học Bách Khoa Tp HCM, 142 Tô Hiến Thành, Quận 10.**

Tel : **22103801**

6. Mắt Bão



Tên công ty: Công ty TNHH Thương Mại Dịch Vụ Mắt Bão

Tên tiếng Anh: Mat Bao Trading and Service Company Limited

Địa chỉ: Tòa nhà Anna, CVPM Quang Trung, P.Tân Chánh Hiệp, Q.12, TP.HCM

Điện thoại: (84.8) 3 868 1888

Fax: (84.8) 35 122 690

Website: www.matbao.com

VPĐD: 334 Cao Thắng, Quận 10, TP.HCM

Lĩnh vực hoạt động:

Dịch vụ tên miền. Cho thuê hosting, máy chủ, trung tâm dữ liệu. Dịch vụ trực tuyến (OSP), Dịch vụ Internet (ISP).

Sản phẩm và dịch vụ:

Cung cấp các giải pháp về phát triển website ứng dụng trên nền web, gồm: thiết kế, lập trình, cung cấp tên miền, máy chủ web và các dịch vụ tư vấn khác về ứng dụng web; cung cấp các giải pháp phát triển ứng dụng phần mềm và thương mại điện tử; cung cấp dịch vụ cho thuê máy chủ, đặt website, phát triển ứng dụng quản lý, một số lĩnh vực khác liên quan đến máy tính, internet và truyền thông đa phương tiện.

7. VIETPACE



GIỚI THIỆU

Trụ sở chính

- Địa chỉ: 36 Đồng Xoài, Phường 13, Quận Tân Bình
- Điện Thoại: +84 8 496 799
- Fax: +84 4 8 4 496 792
- Web : www.vietpace.com / www.baomatoracle.com

Chi nhánh

- Địa chỉ: Tòa nhà SSP, 123 Trương Định, P7, Q3, Tp HCM
- Điện Thoại: +84 8 39.325.977
- Fax: +84 8 9.321.042
- E-mail: contact@vietpace.com

Giới thiệu chung

Được thành lập từ năm 08/05/2006, mục tiêu của VIETPACE là phát triển và trở thành công ty tư vấn, đào tạo và triển khai dịch vụ tin học Oracle hàng đầu ở Việt Nam. Định hướng chuyên nghiệp hoá về tư vấn và phát triển dịch vụ tin học Oracle đó là điểm khác biệt của công ty chúng tôi đối với các công ty khác trong lĩnh vực công nghệ thông tin.

Các hướng dịch vụ và giải pháp mà VIETPACE Co., Ltd. đầu tư và tập trung phát triển là:

1. Tư vấn giải pháp công nghệ Oracle - Sun
2. Giải pháp kiện toàn an ninh hệ thống dữ liệu Oracle tổng thể
3. Giải pháp kỹ thuật Oracle
4. Giải pháp hệ thống dựa trên nền tảng công nghệ SUN và EMC
5. Giải pháp đào tạo chuyển giao công nghệ ORACLE - SUN

Mục tiêu

Với nguồn nhân lực chuyên nghiệp và quyết tâm đem đến khách hàng những dịch vụ chất lượng cao, chúng tôi xác định mục tiêu của mình là trở thành công ty chuyên tư vấn, đào tạo và thực hiện các dịch vụ về Oracle - Sun hàng đầu tại Việt Nam.

Đội ngũ

Đội ngũ của VIETPACE Co., Ltd. là kết hợp chặt chẽ những kỹ sư, lập trình viên và kỹ thuật viên luôn đoàn kết, quyết tâm hoàn thành nhiệm vụ. Chúng tôi tin tưởng sẽ đem đến khách hàng những dịch vụ chất lượng cao, phong cách chuyên nghiệp, vì đội ngũ của chúng tôi là tập hợp của những chuyên gia có :

- ✓ Nhiều năm kinh nghiệm triển khai và vận hành các hệ thống Oracle lớn
- ✓ Quản trị nhiều hệ thống luôn hoạt động 7x24 giờ với dữ liệu rất quan trọng
- ✓ Chứng nhận đẳng cấp quốc tế :
 - o OCP-9i : 3 người
 - o OCP-10g : 2 người
 - o OCP-11g : 2 người
 - o SCSA : 2 người
 - o CCISP : 1 người

Đối tác chiến lược



Tóm tắt giải pháp

Chúng tôi chuyên cung cấp các dịch vụ chuyên nghiệp liên quan đến công nghệ Oracle và Sun với chất lượng tốt nhất, gồm có:

Tư vấn

Với đội ngũ chuyên gia hơn 10 năm kinh nghiệm vận hành và triển khai nhiều giải pháp chuyên nghiệp về công nghệ Oracle – Sun đến nhiều khách hàng lớn, chúng tôi có thể tư vấn:

1. Kiến trúc và giải pháp tổng thể nhằm giúp hệ thống dữ liệu Oracle vận hành an toàn, ổn định và hiệu năng cao nhất
2. Chính sách ATTT trong mạng nội bộ khách hàng và giải pháp giúp kiện toàn bảo mật hệ thống thông tin Oracle của khách hàng

Kiện toàn bảo mật Oracle

Là đối tác của hãng AppSec, được ủy quyền duy nhất tại Việt Nam, chúng tôi tiên phong và duy nhất cung cấp các dịch vụ này tại Việt Nam.

1. Dịch vụ trọn gói về thiết kế và thi công nhóm các giải pháp tổng thể nhằm giúp kiện toàn bảo mật tối đa cho hệ thống thông tin Oracle doanh nghiệp
2. Giải pháp giám sát ghi vết mọi truy cập trái phép trong hệ thống dữ liệu doanh nghiệp
3. Gói giải pháp đánh giá yếu điểm bảo mật Oracle và vá lỗi lỗ hổng nếu có
4. Giải pháp mã hóa dữ liệu trao đổi vào ra hệ thống Oracle

Hỗ trợ kỹ thuật Oracle

1. Phân phối bản quyền giấy phép sử dụng phần mềm Oracle
2. Hỗ trợ kỹ thuật thường niên hệ thống dữ liệu Oracle
3. Dịch vụ thi công kỹ thuật
 - Giải pháp sao lưu và phục hồi dữ liệu bị mất, hư hỏng

- Giải pháp tối ưu tính chỉnh hiệu năng hệ thống dữ liệu Oracle
- Giải pháp chuyển đổi nâng cấp hệ thống Oracle chạy trên IBM, HP-UX, SUN
- Dịch vụ cài đặt các giải pháp RAC, Data Guard, Replication trên IBM, HP-UX, SUN

Giải pháp hệ thống

1. Giải pháp máy chủ
2. Giải pháp lưu trữ dữ liệu

Đào tạo chuyên giao công nghệ

1. Kỹ thuật tấn công và giải pháp chống tấn công hệ thống Oracle
2. Quản trị và phát triển ứng dụng CSDL
3. Quản trị SUN Solaris
4. Các khóa đào tạo cao cấp theo nhu cầu doanh nghiệp

8. VIETUNION CORP

Trụ sở chính:

Lầu 7-9, Tòa nhà 65-65A, Đường 3/2

Phường 11, Quận 10

ĐT: (84-8) 3929 2827

Fax: (84-8) 3929 2826

Văn phòng Hà Nội:

115, Đào Tấn, Quận Ba Đình, Hà Nội.

Website: www.payoo.com.vn

www.vidientu.com.vn

Email: info@vietunion.com.vn



Công ty Cổ phần Dịch vụ Trực tuyến Cộng Đồng Việt - VietUnion là thành viên Tập đoàn Đầu tư Sài Gòn - Saigon Invest Group, tập đoàn kinh tế tư nhân đa ngành hàng đầu Việt Nam. Cổ đông sáng lập của VietUnion là Công ty Cổ phần Công nghệ Viễn thông Sài Gòn (SaigonTel) và Ngân hàng Thương mại Cổ phần Nam Việt (NaviBank), cùng những chuyên gia trong lĩnh vực công nghệ thông tin và quản trị ngân hàng của Tập đoàn Đầu tư Sài Gòn.

Hoạt động trong lĩnh vực Công nghệ thông tin và Thương mại điện tử, VietUnion tập trung cung cấp các giải pháp hỗ trợ giao dịch điện tử và phương tiện thanh toán trực tuyến với định hướng **“Xây dựng một nền tảng giao dịch an toàn và tiện lợi cho sự phát triển của thương mại điện tử tại Việt Nam”**.

Theo đó, hệ thống thanh toán trực tuyến Payoo tại địa chỉ www.payoo.com.vn và www.vidientu.com.vn là một trong những nỗ lực xóa bỏ những rào cản đối với thương mại điện tử Việt Nam hiện nay.

Ví điện tử Payoo cũng là đơn vị đầu tiên tại Việt Nam cung cấp Ví điện tử cho người dùng Internet nhằm hỗ trợ các hoạt động mua – bán và giao dịch trực tuyến tại các trang web thương mại điện tử và tại các cộng đồng mạng có hoạt động thanh toán hoặc trả phí.

Tháng 2/2009, VietUnion được Ngân hàng Nhà nước chính thức cấp phép thí điểm cung ứng phương tiện thanh toán Ví điện tử thông qua các tổ chức cung ứng dịch vụ thanh toán theo Quyết định số 288/QĐ-NHNN.

Tháng 4/2009, hệ thống Ví điện tử Payoo nhận được giải thưởng Sao Khuê 2009 cùng danh hiệu Phần mềm Ưu việt 4 sao do Hiệp hội Doanh nghiệp Phần mềm Việt Nam – VINASA trao tặng.

VIETUNION CORP.

Head Office:

Floor 7th -9th , Building 65-65A, 3/2 Street
Ward 11, Dist 10, Ho Chi Minh City, Vietnam
Tel: (84-8) 3929 2827
Fax: (84-8) 3929 2826

Hanoi Office:

115, Dao Tan street, Ba Dinh, Hanoi
Website: www.payoo.com.vn
www.vidientu.com.vn
Email: info@vietunion.com.vn

VietUnion is a member of Saigon Invest Group (SGI), one of the largest non-state owned groups in Vietnam.

Its founders are Saigon Telecommunication and Technologies Corporation (SaigonTel) and Nam Viet Commercial Joint Stock Bank (NaviBank).

Focusing on Information Technologies and e-Commerce, VietUnion provides resolutions to electronic transactions and payment means for Banking in e-commerce in order to **“build up the safe and convenient transaction bases supporting to the development of e-commerce in Vietnam”**. And Payoo e-wallet, the new online payment service built up by VietUnion, is one of its efforts to overcome barriers which exist in Vietnam’s e-commerce.

VietUnion is also a provider of the first e-wallet service in Vietnam to support e-commerce websites and e-communities in online payment transaction.

VietUnion is one of the four businesses licensed to perform the pilot provision of payment means of Payoo EWallet through Payment Services Organization by The State Bank (Decision No 288/QĐ-NHNN, 18/02/2009).

Payoo E-Wallet has won Sao Khue 2009 Award and the title of 4-star Preeminent Software chosen and announced on 24/04/2009 by VINASA.

9. NTS Group



Với lịch sử phát triển gần 11 năm 1998 - 2009, NTS Group mang đến cho hàng triệu khách hàng tại Việt Nam những sản phẩm công nghệ hàng đầu thế giới để cùng nhau tạo ra tiện nghi sống và làm việc tốt hơn cho người Việt Nam. NTS Group hiện nay, bao gồm 09 công ty thành viên: NTS ICT, NTSD, NTS SI, NTS Training, NTS Hà Nội, NTS Đà Nẵng, NTS Cần Thơ, NTS Security, NTS Media.

Các thương hiệu nổi bật của NTS Group: KASPERSKY LAB, ASTARO, ZYXEL, SOURCEFIRE, INFOGUARD, IPOGUE và KAX.

Sứ mệnh – Mục tiêu:

Sứ mệnh của chúng tôi là gia tăng những giá trị mới, phát triển bền vững cùng với các đối tác tại Việt Nam và trên Thế Giới. Chúng tôi quan tâm đến nhu cầu tiện nghi công nghệ hàng ngày của người Việt Nam và phát triển các ứng dụng công nghệ mới thông qua các thương hiệu đáp ứng tốt hơn và tốt nhất các nhu cầu đó.