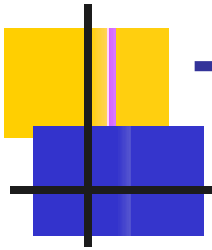
AN NINH MẠNG

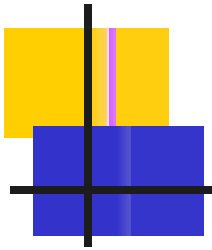
Biên soạn : HUỲNH THANH HÒA

cuu duong than cong. com

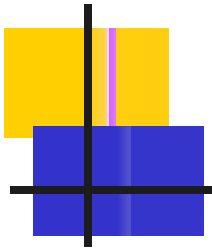


Tổng quan về an toàn bảo mật.

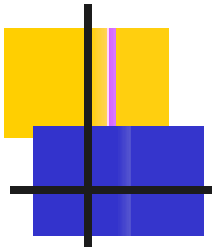
- An toàn hệ thống thông tin là gì ?
- Mục tiêu bảo vệ hệ thống thông tin.
- Các yêu cầu an toàn bảo mật hệ thống thông tin : có 4 yêu cầu chính



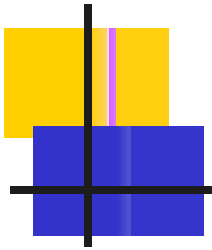
- Đảm bảo tính tin cậy(*Confidentiality*): Thông tin không thể bị truy nhập trái phép bởi những người không có thẩm quyền.
- Đảm bảo tính nguyên vẹn(*Integrity*): Thông tin không thể bị sửa đổi, bị làm giả bởi những người không có thẩm quyền.



- Đảm bảo tính sẵn sàng(*Availability*): Thông tin luôn sẵn sàng để đáp ứng sử dụng cho người có thẩm quyền
- Đảm bảo tính không thể từ chối (*Non-repudiation*): Thông tin được cam kết về mặt pháp luật của người cung cấp.



- Các nguyên tắc cơ bản khi thiết kế các giải pháp bảo vệ hệ thống thông tin.
- Các bước xây dựng "chương trình bảo vệ thông tin" : có 6 bước



- Xây dựng chính sách an toàn thông tin (Policy).
- Phân tích rủi ro trong hệ thống thông tin (Risk Analysis).
- Xây dựng các biện pháp phòng chống (Prevention).
- Xây dựng các biện pháp phát hiện (Detection).
- Xây dựng các biện pháp đáp ứng - phản ứng (Response).
- Xây dựng "văn hoá" cảnh giác (Vigilance).

Xây dựng chính sách an toàn thông tin

- **Bộ chính sách ATTT nhằm xác định**: Confidentiality (Tính bảo mật), Integrity (Tính toàn vẹn), Availability (Tính sẵn sàng).

Ví dụ: một chính sách ATTT

Loại thông tin	Tính bí mật	Tính toàn vẹn	Tính sẵn sàng cao
Chiến lược kinh doanh	✓	✓	
Thông tin tài chính nội bộ	✓	✓	✓
Tình hình nộp thuế		✓	
…			

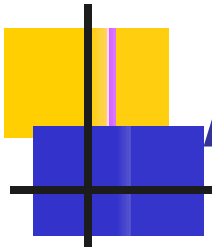
Phân tích - đánh giá rủi ro

- Các mối đe doạ (Threats).
- Các điểm yếu (Vulnerabilites).
- Các rủi ro (Risk).

$$Risk = \sum_{Thread=1}^{n} (\text{Asset Value} * \text{Probability})$$

Trong đó:

- Risk: Tổng rủi ro.
- Asset value: Giá phải trả khi phải thay thế tài sản.
- Probability: Xác suất đe doạ xảy ra đối với một tài sản.



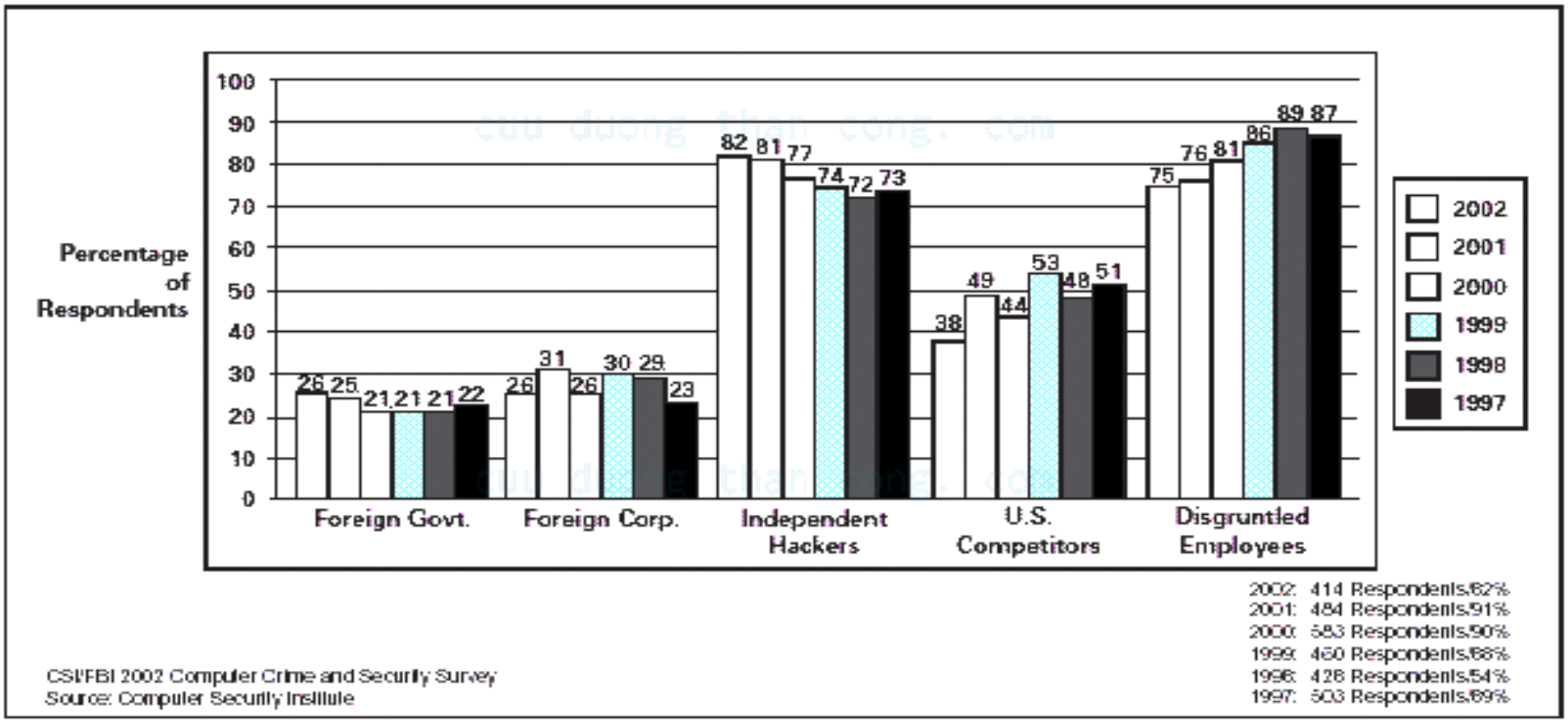
Hiện trạng an toàn bảo mật.

- Nhận thức và đầu tư cho Security.

cuu duong than cong. com

Mục tiêu và nguồn gốc của tấn công

Likely Sources of Attack



Thiệt hại.

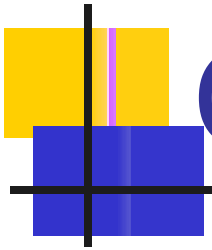
	No of Respondents			Highest Lost ($)		
	2000	2001	2002	2000	2001	2002
Theft of proprietary info	22	34	41	25M	50M	50M
Sabotage of data of networks	28	26	43	15M	3M	10M
Telecom eavesdropping	15	16	20	500K	500K	5M
System penetration by outsider	29	42	70	5M	10M	5M
Insider abuse of Net access	91	99	103	15M	10M	10M
Financial fraud	34	21	40	21M	40M	50M
Denial of Service	46	35	75	5M	2M	50M
Spoofing	n/a	n/a	n/a	n/a	n/a	n/a
Virus	162	186	188	10M	20M	9M
Unauthorized insider access	20	22	31	20M	5M	1.5M
Telecom fraud	19	18	31	3M	8M	100K
Active wiretapping	1	0	0	5M	0	0
Laptop theft	174	143	145	1.2M	2M	5M

- Tính trung bình số tiền thiệt hại của các tổ chức, doanh nghiệp và các dịch vụ được thống kê trong bảng dưới đây:

	Average Losses ($)		
	2000	2001	2002
Theft of proprietary info	3,032,818	4,447,900	6,571
Sabotage of data of networks	969,577	199,350	541,000
Telecom eavesdropping	66,080	55,375	1,205,000
System penetration by outsider	244,965	453,967	226,000
Insider abuse of Net access	307,524	357,160	536,000
Financial fraud	1,646,941	4,420,738	4,632,000
Denial of Service	106,717	122,389	297,000
Spoofing	n/a	n/a	n/a
Virus	180,092	243,845	283,000
Unauthorized insider access	1,124,725	275,636	300,000
Telecom fraud	212,000	502,278	22,000
Active wiretapping	5M	0	0
Laptop theft	58,794	61,881	89,000

- Tổng số tiền thiệt hại hàng năm của các tổ chức doanh nghiệp được thống kê trong bảng sau:

	Total Annual Losses ($)		
	2000	2001	2002
Theft of proprietary info	66,708,000	151,230,100	170,828,000
Sabotage of data of networks	27,148,000	5,183,100	15,134,000
Telecom eavesdropping	991,200	886,000	6,015,000
System penetration by outsider	7,104,000	19,066,600	13,055,000
Insider abuse of Net access	27,984,740	35,001,650	50,099,000
Financial fraud	55,996,000	92,935,500	115,753,000
Denial of Service	8,247,500	4,283,600	18,370,500
Spoofing	n/a	n/a	n/a
Virus	29,171,700	45,288,150	49,979,000
Unauthorized insider access	22,554,500	6,064,000	4,503,000
Telecom fraud	4,028,000	9,041,000	346,000
Active wiretapping	5,000,000	0	0
Laptop theft	10,404,300	8,849,000	11,766,500
Total Annual losses	265,586,240	377,828,700	455,848,000



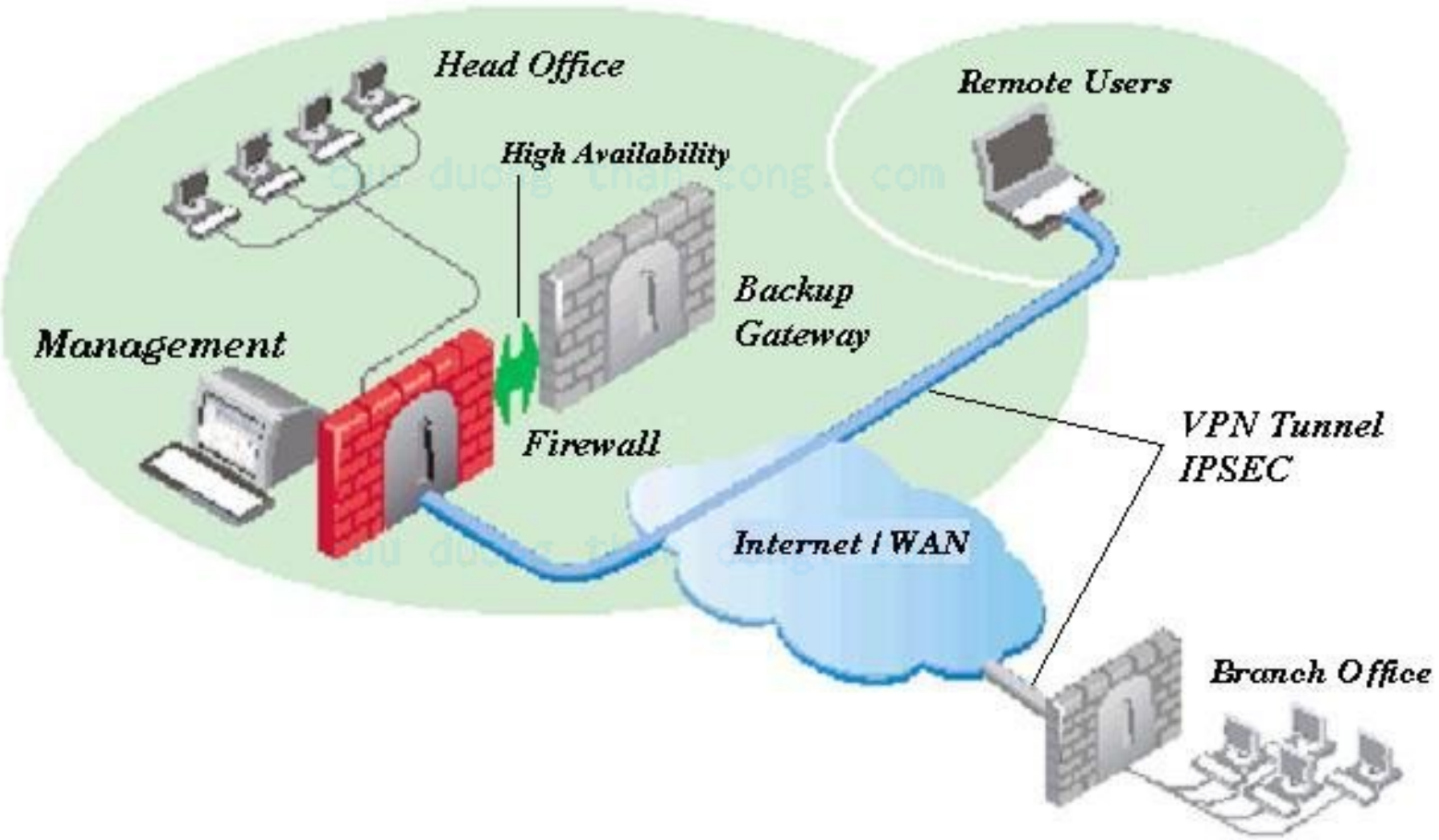
Các kiểu tấn công và thiệt hại

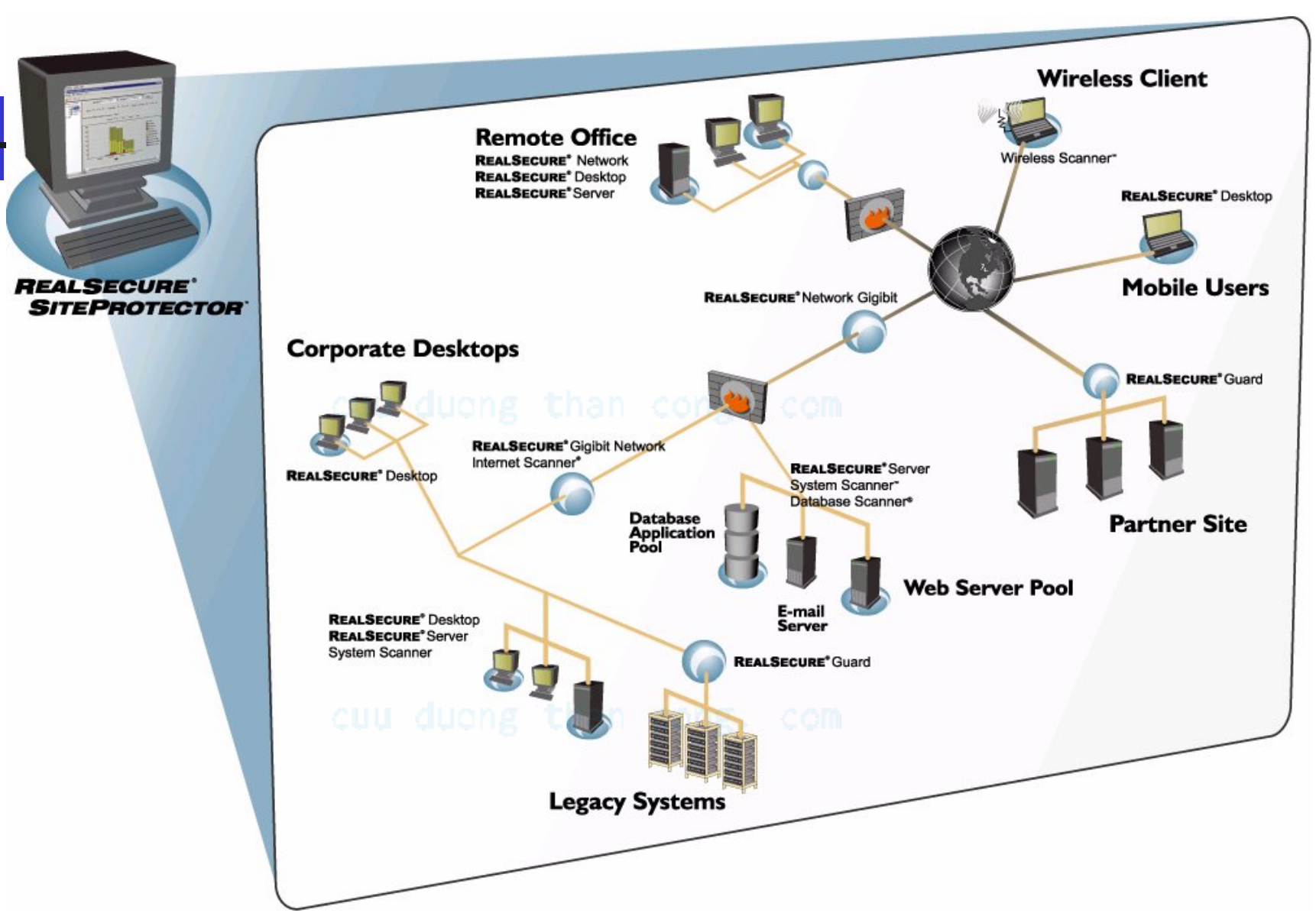
- Denial of Service
- Virus
- Unauthorized insider access

Các công nghệ được lựa chọn

- Bức tường lửa (Firewall)
- Phòng chống virus
- Bảo vệ vật lý
- hệ thống phát hiện xâm nhập (IDS).

* Mô Hình Bảo Mật





THANKS