
A Return On Investment from Computer Security Technology

16th Annual Computer Security
Applications Conference
December 11-15, 2000

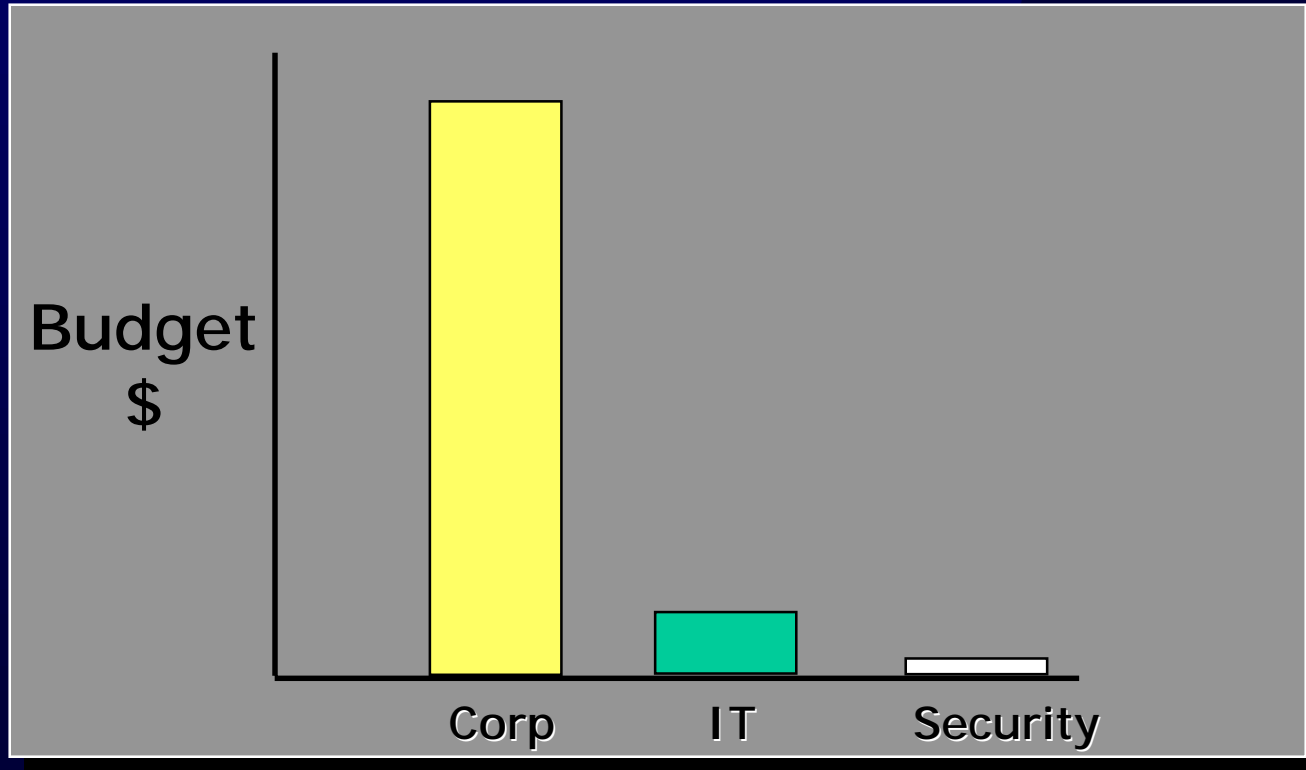
Gregory B. White, Ph.D.
VP Professional Services
SecureLogix Corporation

Strategies to Justify Your Security Budget

What are the Issues?

- How can we secure our systems?
- How do we justify spending money on security?
- Security is generally considered a necessary evil -- something we learn to put up with.
- Security costs but doesn't provide a tangible product and generally doesn't enhance a product either.
- The goal is usually to spend as little on security as possible.
 - Too much security is a waste, not enough can mean trouble.
 - The challenge is to find that fine line between the two.
- The dream -- "Wouldn't it be nice if security paid for itself?"

What are the Issues?



IT Saves

- Duramet Corp., \$10M manufacturer of powdered metal -- an inventory management system helped double sales without increasing the sales force
- Wierton Steel Corp. -- a production line running on a RISC server lets 12 employees run a "hot mill" pressing molten steel that before took 150 people
- Alliance Benefits & Compensation LLC, a health-insurance consulting firm -- uses an application to track sales calls, scheduling, and other tasks which has reduced each salesperson's work time by 2.5 hours/day.

» From "It's Official: IT Adds Up", Informationweek, April 17 2000, p. 42.

A Return on the Investment?

- Security ROI
 - Traditional
 - Improved Security
- General (financial) ROI
 - Budgetary Savings
 - Increase Revenue

Traditional Security ROI

- You have to have security, or else...
 - FUD -- Fear, Uncertainty, Doubt
- Provides a “non-financial” ROI
- A sunk cost, does not provide revenue.

You have to have security, or else...

- 1999 *Information Security Survey*
 - 745 *Information Security Readers*
 - 23% reported unauthorized access from outsiders
 - 91.6% increase over 1998 results
 - 52% reported access abuse by employees
 - 14% reported access abuse by business partners, resellers, or vendors
 - Total loss for 91 reporting a loss was \$23,323,000
 - Average loss \$256,297
 - Security Technologies used
 - Firewalls: 82%
 - Access Controls: 77%

You have to have security, or else...

- 2000 *Information Security Survey*
 - 1897 “infosecurity professionals”
 - 37% experienced a denial of service attack
 - 25% experienced breaches due to insecure password
 - 24% experienced breaches due to buffer overflows
 - 24% experienced attacks on bugs in web servers
 - 58% experienced employee abuse of access controls
 - up from 52% in 1999
 - 24% experienced electronic theft, sabotage or intentional destruction/disclosure of proprietary data or information by employees
 - up from 17% in 1999

You have to have security, or else...

- 1999 CSI/FBI Computer Crime and Security Survey
 - 521 security “practitioners” in the U.S.
 - 30% reported system penetrations from outsiders
 - an increase for the third year in a row
 - 55% reported unauthorized access from insiders
 - also an increase for the third year in a row
 - Losses due to computer security breaches totaled (for the 163 respondents reporting a loss) \$123,779,000
 - Average loss \$759,380
 - Security Technologies used
 - Anti-virus Software: 98%
 - Access Control Mechanisms: 93%
 - Firewalls: 91%

You have to have security, or else...

- 2000 CSI/FBI Computer Crime and Security Survey
 - 643 security “practitioners” in the U.S.
 - 90% reported computer security breaches within the previous 12 months
 - 70% reported unauthorized use
 - 74% suffered financial losses
 - Losses due to computer security breaches totaled (for the 273 respondents reporting a loss) \$265,589,940
 - Average loss \$972,857

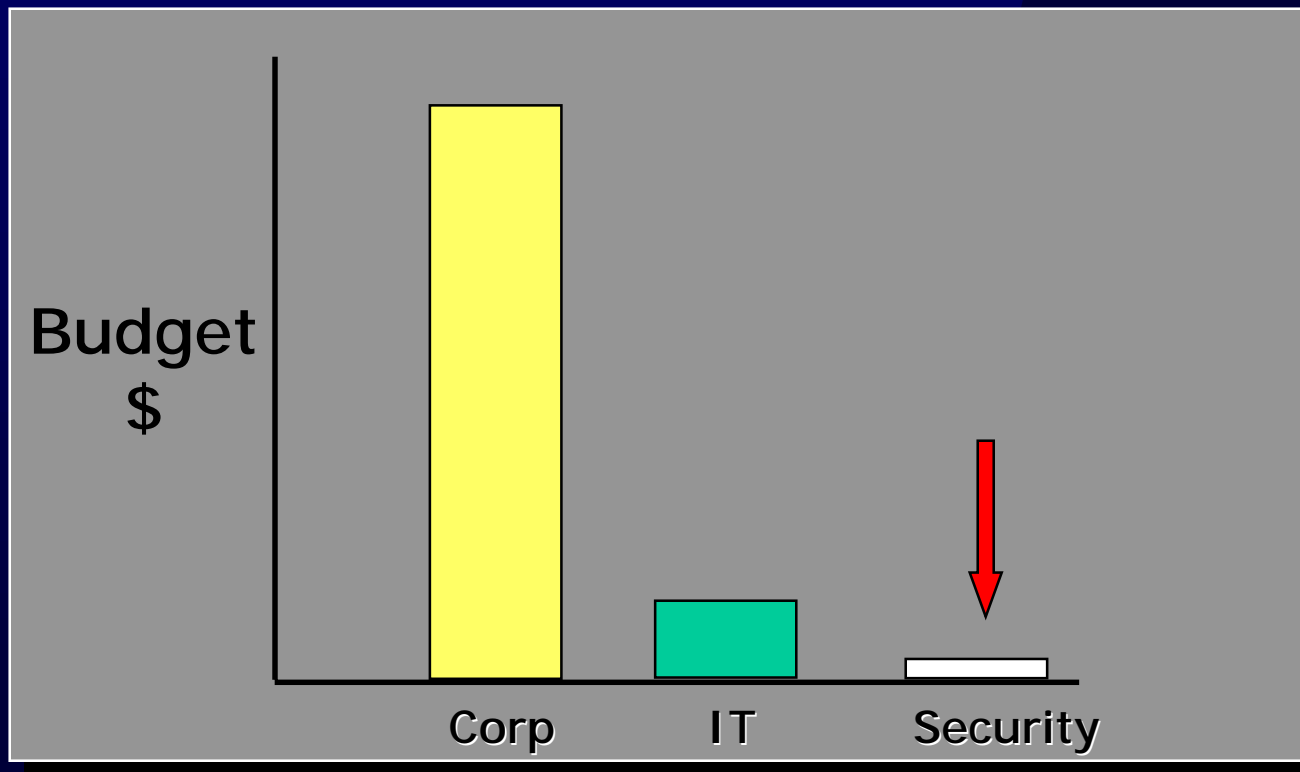
You have to have security, or else...

- Corporate officers can be held accountable for
 - Failure to Protect against loss
 - Failure to Protect against Disclosure
 - Failure to Protect against Harassment
- HIPAA

Improved Security ROI

- I have a limited security budget, I want to be able to do more with it.
 - More “bang for the buck”
 - Leverage money and personnel
- Benefits here limited to the Security budget.

Improved Security ROI



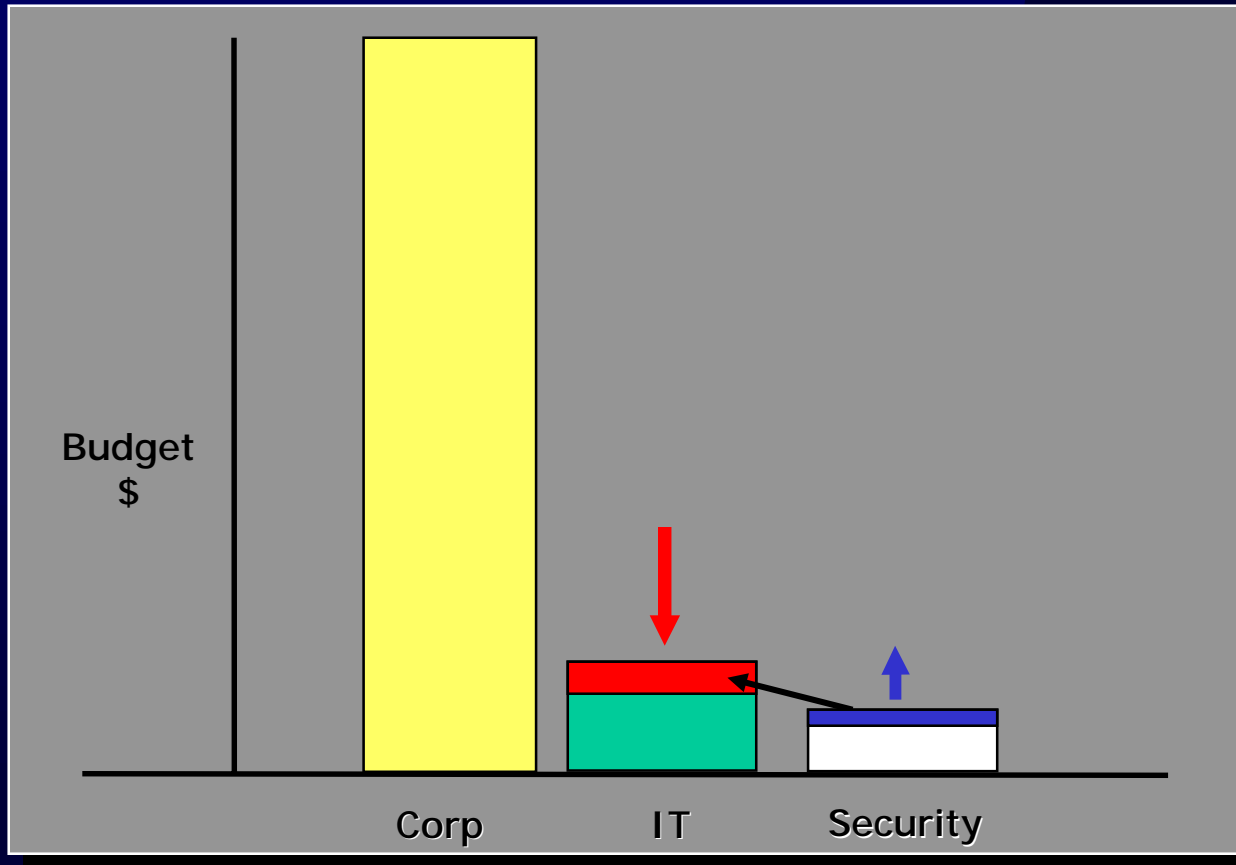
Lessons from the Y2K Aftermath

- Lots of money spent on Y2K preparation
- Many expected the budgets set aside for IT to handle Y2K to be set aside for security once Y2K over with
- We have NOT seen this happen. Why?

General ROI

- Provide savings elsewhere
 - (Budgetary Savings)
- Security as a Business Enabler
 - (Increased Revenue)

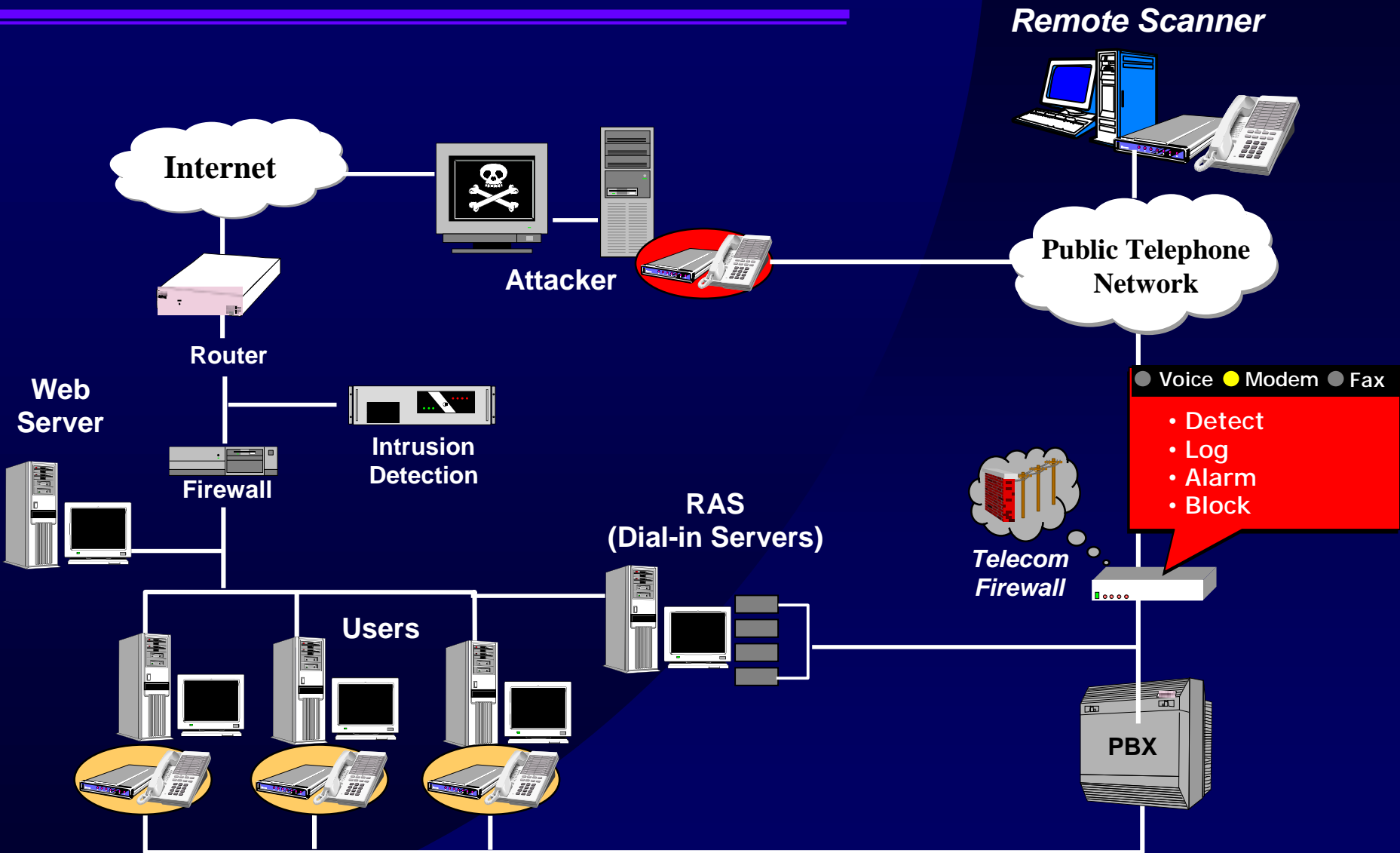
Provide savings elsewhere



Risk Analysis

$$\text{RISK} = \frac{\text{Threat X Vulnerability}}{\text{Countermeasures}} \times \text{Value}$$

The Newer Security Technologies



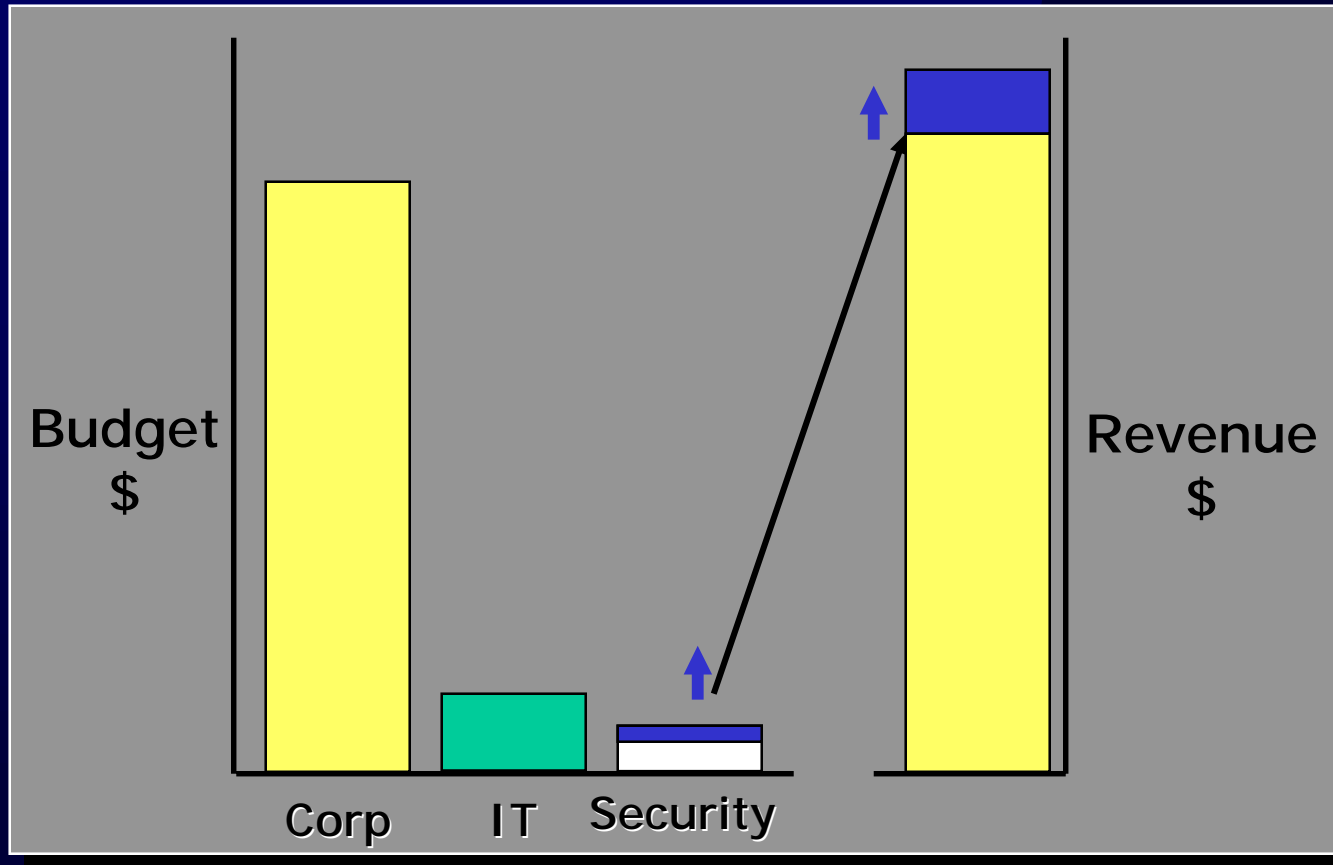
ROI from newer security technologies

- Close the BIG BACK DOOR!
- Control & Forecast Resource utilization
 - How many fax lines do you REALLY need?
- Telephone Bill Reconciliation and Toll Fraud
 - Greyhound recovered over \$1M through an audit of the company's phone bill in 1998
 - Charged for 900 and 3rd party calls
 - "Slamming" (switching long distance carriers without consent)
 - Charged for services not requested or provided elsewhere
 - Toll fraud accounted for \$5B in losses in U.S. in 1999

Business Enabler

- Security allows me to do something I couldn't do [safely] otherwise/before.
 - Electronic Commerce
 - On-line banking
 - On-line Brokers
- Added value, security is part of the product.
 - help make sale because of security
 - revenue generated as a result of the security
- Security is not the product -- it allows me to do business.

Business Enabler



Summary

- Security budget, while growing, will never be a large portion of any organization's budget.
- Security is essential, even if it doesn't result in additional revenue or save money elsewhere.
- Security may provide benefits in terms of increased capabilities not directly related to revenue generation.
- The newest emerging security technologies actually show a promise of providing a true ROI by providing visibility and control of the corporate telephone network.
- If you are trying to justify your security budget on the results of a risk assessment alone, you are in for an uphill battle.