



Obtaining an ROI with Telecommunication Firewalls

Gregory B. White, Ph.D.
Technical Director,
Center for Infrastructure Assurance and Security

17th ACSAC
New Orleans, LA
12 December 2001

UTSA College of Business



The Center for Infrastructure Assurance and Security



- ◆ Consortium of industry, academia, government
- ◆ Dedicated to helping secure the nation's infrastructures
 - “Infrastructure Protection begins in Mineola, not Washington D.C.”

UTSA College of Business



Information Systems Security

-- September/October 2001

- ◆ “Executives Need to Know: The Arguments to Include in a Benefits Justification for Increased Cyber Security Spending”
 - “What is a ‘pound of security’ worth? How can security expenses be justified? Rather, these are not new questions that are only now being raised by the Internet generation. These are questions that have been asked for at least 30 years and, to date, the answers have been less than complete. This shortcoming is apparent because the first complaint usually registered by any computer security official is a lack of adequate funding, whereas the complaint registered most often by funding officials is that the cost-benefit analysis required to accompany requests for security dollars is weak to nonexistent.”

UTSA College of Business



The Quantifiable Argument

- ◆ “Historically, the answer to the question about the worth of a pound of security has been that the cost to secure a computing asset should be less than the annualized replacement cost of the asset should it be destroyed, stolen, or lost.”
- ◆ “the difficulty of developing a realistic benefits justification for increased cyber security spending cannot be fully resolved until some standard metrics are devised to address the valuation problem.”

UTSA College of Business



Nonquantifiable Arguments

- ◆ Cost of conducting E-Business
 - Security is simply a cost of doing business
- ◆ Loss of Revenue Due to Security Breaches
 - Loss per hour estimates:
 - Financial Institutions \$2-6M
 - Retail \$100-150K
 - Transportation (airline reservations) \$90K
- ◆ Supply Chain Responsibilities
 - Links to business partners (weak-link concept)
- ◆ Loss of Business Opportunities
 - Because of privacy concerns, if you aren't secure customers won't do business with you
- ◆ Obligations to the National CIP effort

UTSA College of Business



Design Criteria for a Successful Cyber Security Program

- ◆ Adopt a balanced strategy
 - Prevention, detection, and response
 - Operational Model – pioneered in AF in late 80's
- ◆ A management process is needed to administer security.
 - A plan-fix-monitor-assess cycle
- ◆ Design to due diligence standards

UTSA College of Business



Putting it all together

- ◆ Assemble an Executive-level cyber security decision team.
- ◆ Assure the security initiatives conform to the criteria for a successful program
- ◆ Assure that National or International guidelines for cyber security programs are followed.
- ◆ Identify and value quantifiable assets
- ◆ Identify and value nonquantifiable assets and processes
- ◆ Identify reputation and value factors
- ◆ Summarize benefits of increased security and determine a due diligence course of action

UTSA College of Business



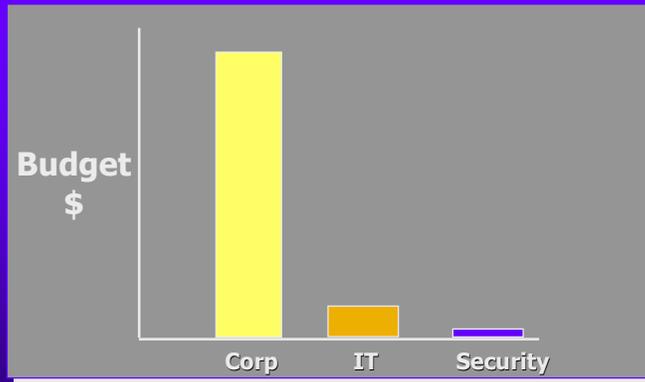
Computer/Network Security: What are the Issues?

- ◆ 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 accept.
- ◆ Security costs but doesn't provide a tangible product and generally doesn't enhance a product either.
- ◆ The goal is to spend as little on security as possible.
 - Too much is a waste, not enough can mean trouble.
 - The challenge: to find that fine line between the two.
- ◆ The dream -- "Wouldn't it be nice if security paid for itself?"

UTSA College of Business



What are the Issues?



UTSA College of Business



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.

UTSA College of Business



A Return on the Investment?

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

UTSA College of Business



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.
 - Does it have to? Is there still value even if it doesn't provide a financial ROI?

UTSA College of Business



Non-financial ROI

“Financial measurements alone are seldom sufficient to support decisions with long-term impact. Managers must consider the financial return of an IT investment in relationship to other factors such as risk, feasibility and the long-term goals of the organization.”

-- CIO Council Capital Planning and
IT Investment Committee

UTSA College of Business



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%

UTSA College of Business



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%

UTSA College of Business



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

UTSA College of Business



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

UTSA College of Business



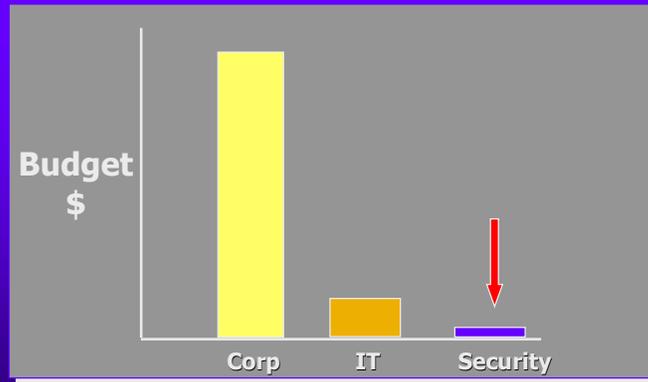
Improved Security ROI

- ◆ 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.

UTSA College of Business



Improved Security ROI



UTSA College of Business



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?

UTSA College of Business



General ROI

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

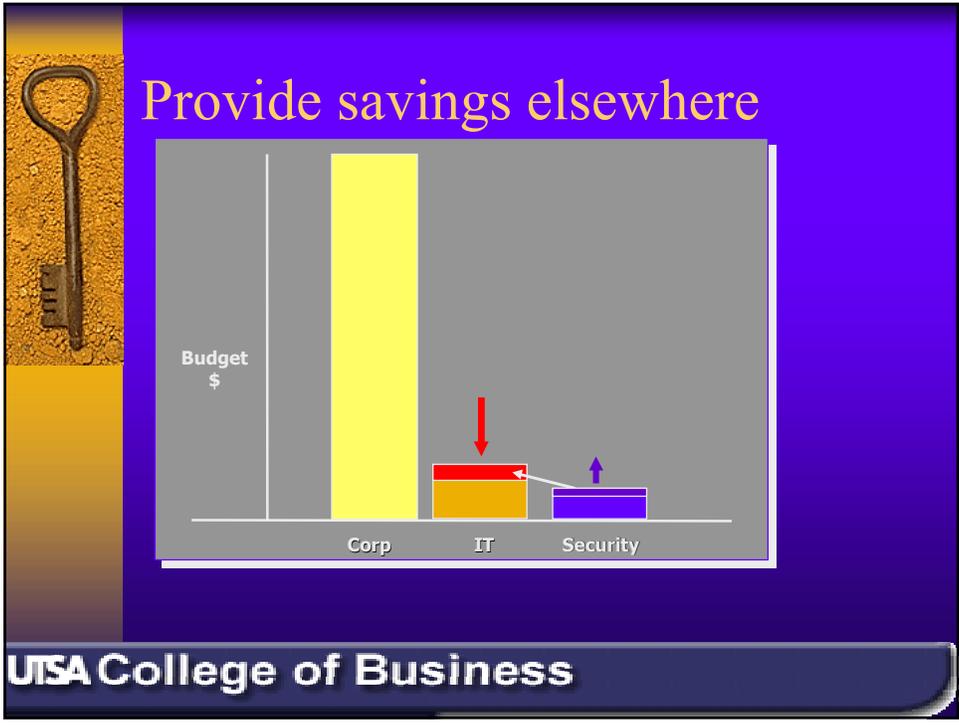
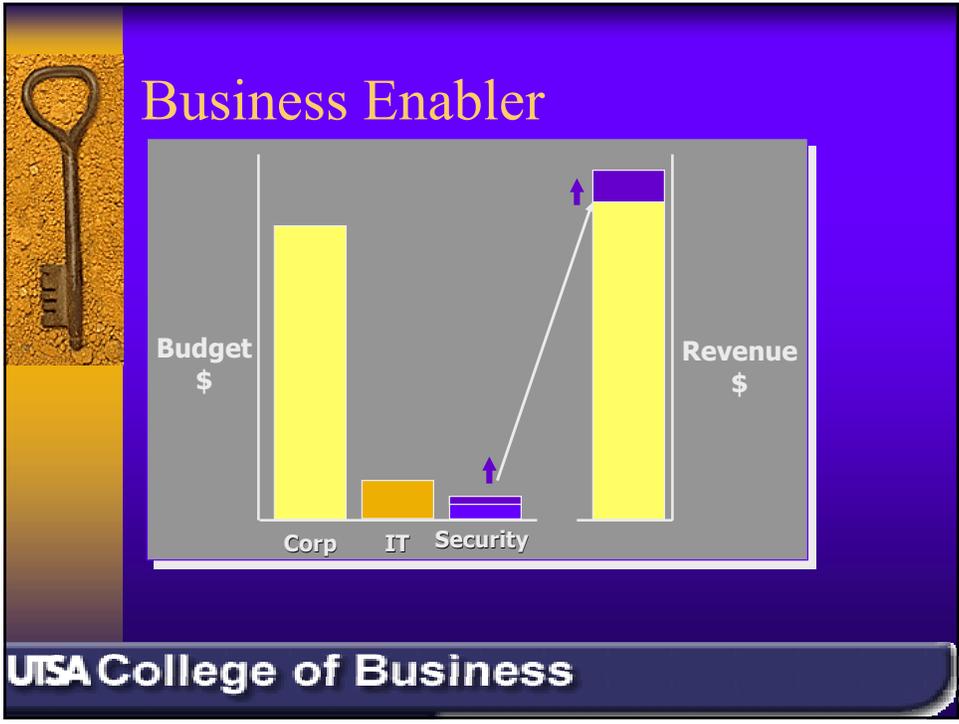
UTSA College of Business



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.

UTSA College of Business

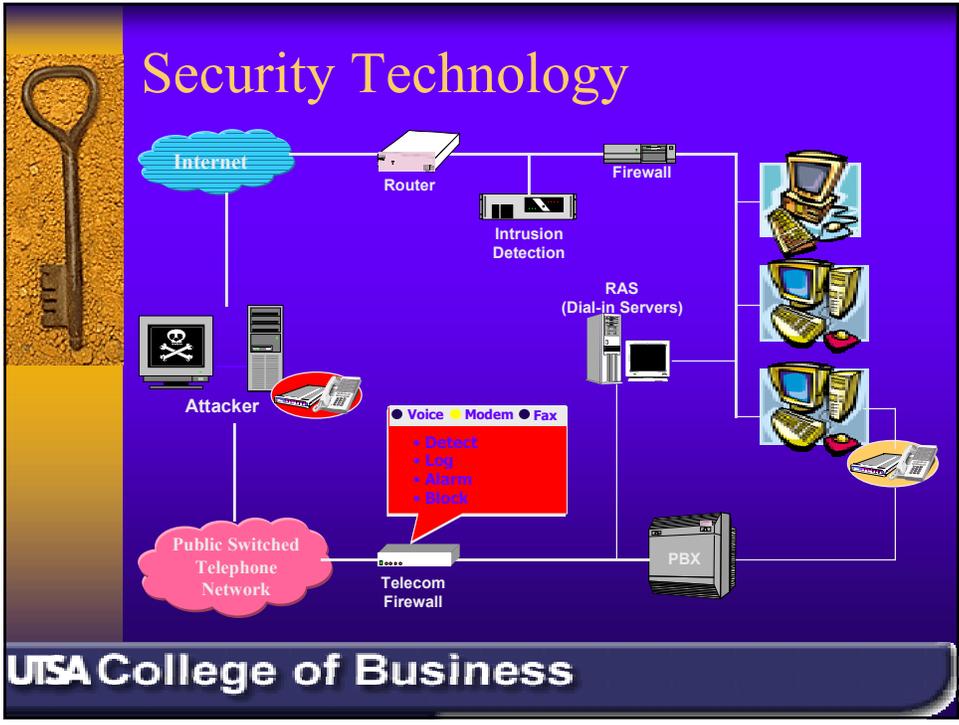




Risk Analysis

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

UTSA College of Business





Visibility & Control

- ◆ What the newer security technologies provide is visibility and control
 - Corporate Network Structure
 - Corporate Data Stream
 - Provides an enterprise-wide view of exactly what is happening in the corporate network, AND
 - Provides an ability to control it.

UTSA College of Business



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

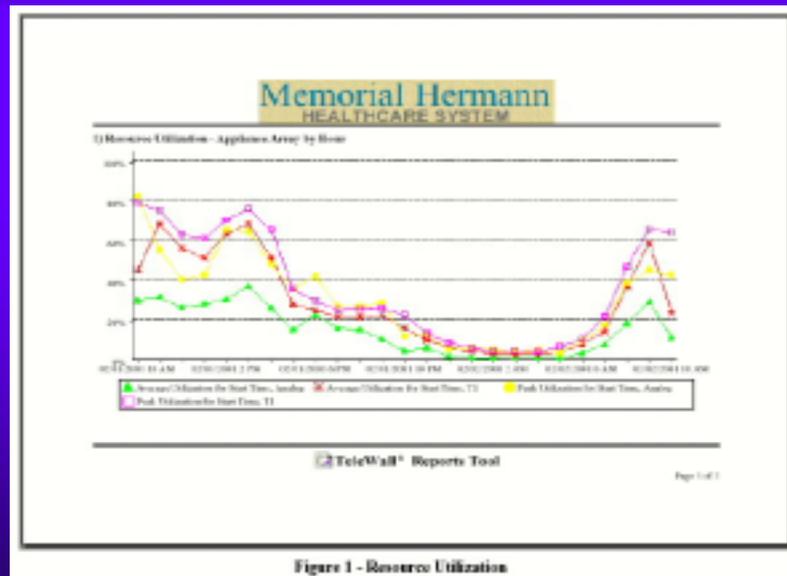
UTSA College of Business



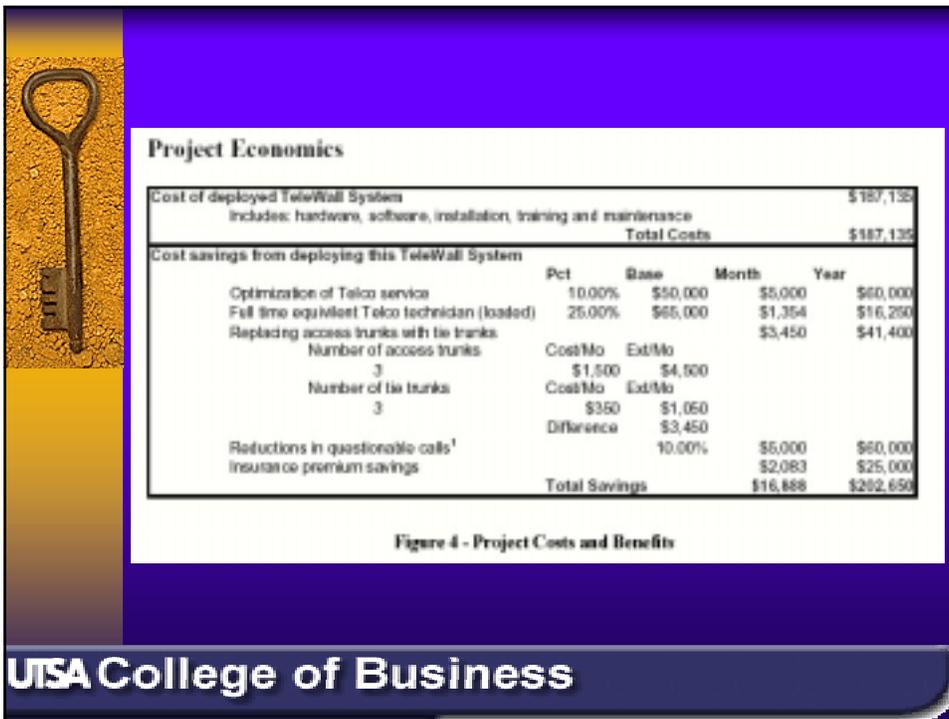
Case Study using TeleWall TFW

- ◆ Hermann Memorial Hospital
- ◆ December 2000 Test
 - 17 T-1's, 4 Analog sensors
- ◆ Results
 - Optimization of Telephony Service Capacity
 - Reduction in Full time equivalent (FTE) employee costs
 - Eliminate unauthorized modems accessing local ISP's
 - Replacement of expensive local access trunks with more cost-effective tie-trunks
 - Recovered capacity from reductions in inappropriate use
 - Insurance premium savings

UTSA College of Business



UTSA College of Business



UTSA College of Business



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.

UTSA College of Business