IPCOMM2006

September 25-27 • Gaylord Opryland • Nashville, TN

Chaos to Simplicity: Making Sense of the Security Marketplace

Paul Adamonis
Director, Security Solutions
Forsythe

What Will Be Covered

Market Trends
What Security Vendors Do
Security Vendor Framework
IPT Security Measures

Definition of Chaos

Webster Definition

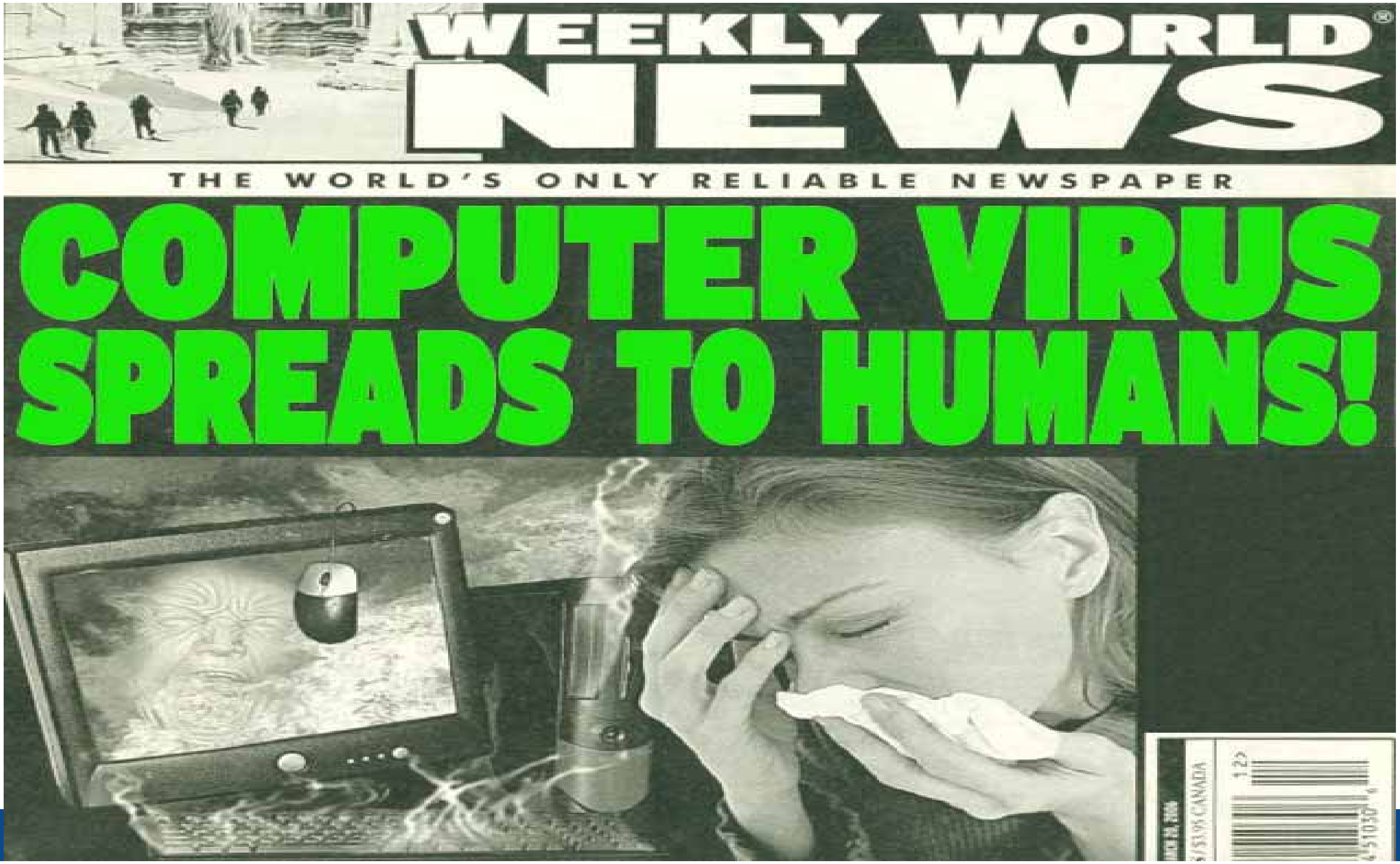
Chaos: (kā´ŏs) n. A State or place of total confusion and disorder.

Conventional Wisdom

KAOS: Killing and Other Stuff

HIPAA
SOX
ISO 17799
COBIT
GLBA
FDA
IRS
SEC
Visa CISP/PCI
Identity Theft
Privacy Law
ITIL

Market Trend



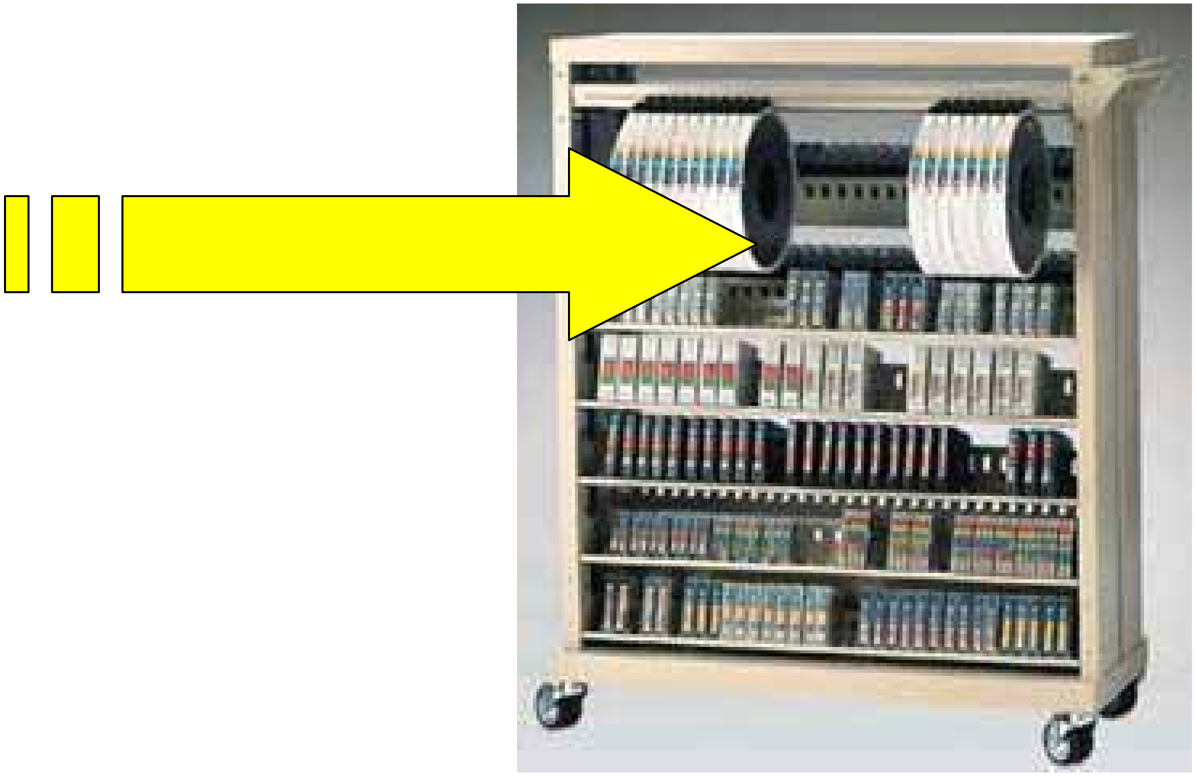
WEEKLY WORLD NEWS

THE WORLD'S ONLY RELIABLE NEWSPAPER

COMPUTER VIRUS SPREADS TO HUMANS!

Market Trend

Information Security is dependent on Physical Security



Tapes are missing!!

“My laptop was stolen!”

Market Trend

2006 Breaches in the news

- May 22 – Department of Veterans Affairs
  - 28.6 Million Veterans
- June 2006 – Net2Phone VoIP Scam
  - Millions in revenue, 15 companies affected
- June 2 – YMCA, Providence RI
  - 65,000 members with health information
- July 5, - Bisys Group, Roseland NJ
  - 61,000 hedge fund investors

Total number of Individuals affected since Feb 15, 2005

Over 88 Million!!

Typical Company Response

We have to do something NOW!

- Stop the bleeding – Respond to Chaos
- Identify the issues – Determine need
- Research vendor solutions
- Square peg into a round hole
- Add management to someone’s role

Band Aids and Solutions

- Anti-Spam
- Two Factor Authentication
- Spyware
- Patch Management
- IM Content Control
- Endpoint Security
- Email Encryption
- File Encryption
- URL Filtering
- Security Event/Incident Management
- Intrusion Prevention
- Media/Tape Encryption

- Biometrics
- Data Loss Prevention
- Single Sign On
- Firewall
- VPN
- Anti-Virus
- Integrated Appliances
- Application Firewalls
- Database Encryption
- SSL VPN
- Compliance Monitoring
- Wireless
- Identity Provisioning
- Storage Encryption

AND MORE!

MRV
Akonix
Solutions for Enterprise IM
Cisco Systems
Infoblox
Network Instruments
McAfee
F5
Vericept
NetScaler
Blue Coat
eEye Digital Sec
Tron
Qualys
Security On Demand
Secure Computing
PassGo
Ingrian Networks
blues
The leader in
Nokia
Connecting People
WholeSecu
behav
Juniper
Check Point
Software Technologies Ltd.
We Secure the Internet.
RDEDNET
SECURING PRODUCTIVITY
TippingPoint
RSA
Security
SurfConti
Trend Micro
symantec.
SECURING THE GLOBAL VILLAGE
Sourcefire
Security for the real world.
AirMagnet
Internet Security Systems
radware
ailability | performance | security
Funk Software
Decru
Securing Networked Storage
NetScout

Security Vendor Consolidation

$16 Billion Security market

Remove the top 5-10 vendors

Left with $12 Billion over 600 vendors

= $20 million per vendor

Result: Departures and Convergence

RSA Security bought by EMC

CipherTrust Merges with Secure Computing

ISS rumored to be bought by IBM

Point to Ponder

“I do not think that the wireless waves I have discovered will have any practical application”

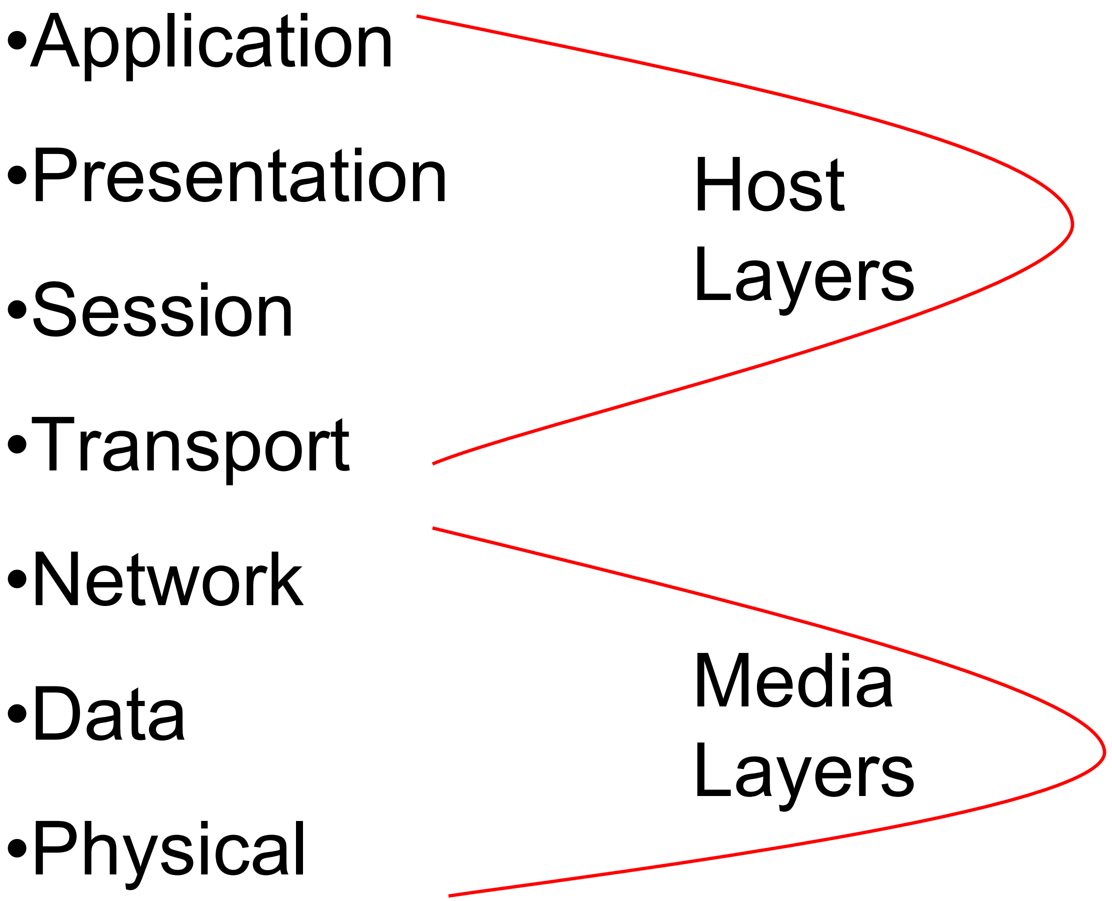
Heinrich Rudolf Hertz

Security Vendor Framework

- Why is it needed
- Proper Approach
- Value of structured approach

Categorize the Need

- Advice
- People’s
- Sales
- Take
- Not
- Do
- Please

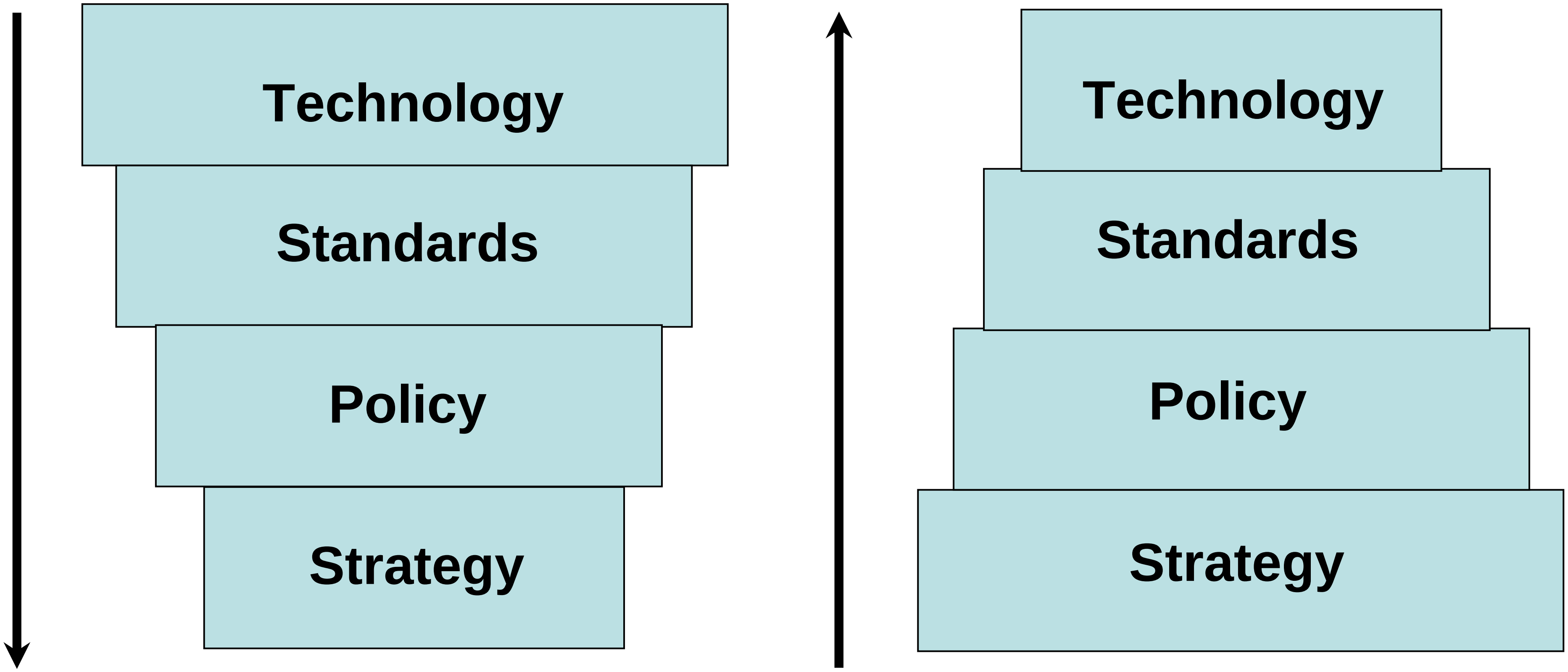


- Application
- Presentation
- Session
- Transport
- Network
- Data
- Physical

Host Layers

Media Layers

Turning the Security Program Rightside Up



Technology

Standards

Policy

Strategy

Technology

Standards

Policy

Strategy

Where Do Enterprises Start?

Security Assessments: *set a baseline*

Identify risks, threats, vulnerabilities, current state, define strategy

Security Program: *make a statement*

Charter, Policy, Standards, Procedures, Guidelines

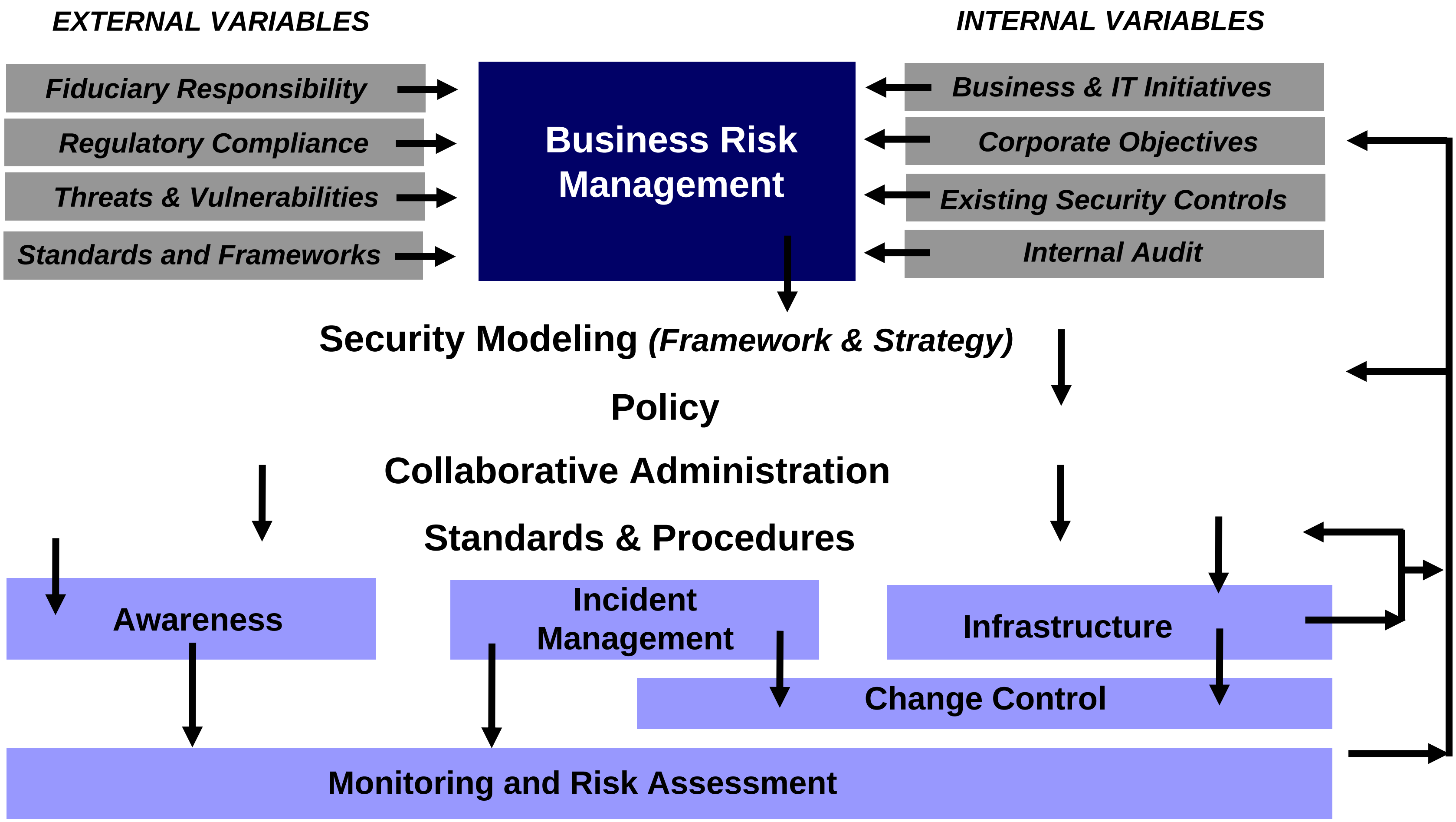
Awareness and training, user education

Security Architecture: *apply technology*

Solutions and products for specific security areas

Monitoring, detection and incident response

Information Security Governance



EXTERNAL VARIABLES

- *Fiduciary Responsibility*
- *Regulatory Compliance*
- *Threats & Vulnerabilities*
- *Standards and Frameworks*

INTERNAL VARIABLES

- *Business & IT Initiatives*
- *Corporate Objectives*
- *Existing Security Controls*
- *Internal Audit*

Business Risk Management

Security Modeling *(Framework & Strategy)*

Policy

Collaborative Administration

Standards & Procedures

Awareness

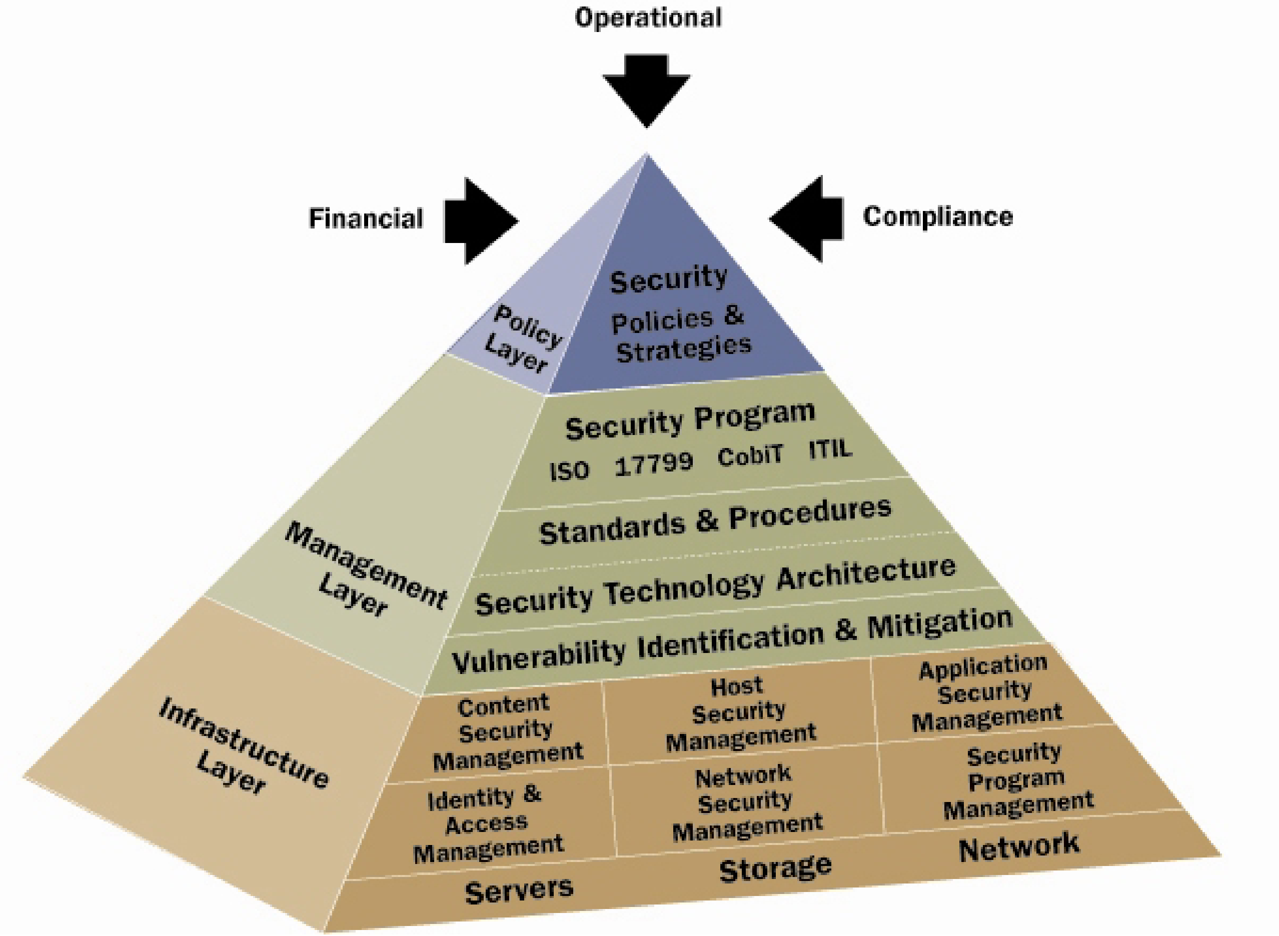
Incident Management

Infrastructure

Change Control

Monitoring and Risk Assessment

Solid Security Approach


Operational
Financial
Compliance
Policy Layer
Security Policies & Strategies
Management Layer
Security Program
ISO 17799 CobiT ITIL
Standards & Procedures
Security Technology Architecture
Vulnerability Identification & Mitigation
Infrastructure Layer
Content Security Management
Host Security Management
Application Security Management
Identity & Access Management
Network Security Management
Security Program Management
Servers
Storage
Network

Categorize Your Vendors

- Anti-Spam
- Two Factor Authentication
- Spyware
- Patch Management
- IM Content Control
- Endpoint Security
- Email Encryption
- File Encryption
- URL Filtering
- Security Event/Incident Management
- Intrusion Prevention
- Media/Tape Encryption
- Biometrics
- Data Loss Prevention
- Single Sign On
- Firewall
- VPN
- Anti-Virus
- Integrated Appliances
- Application Firewalls
- Database Encryption
- SSL VPN
- Compliance Monitoring
- Wireless
- Identity Provisioning
- Storage Encryption

Current Security Technologies

- Anti-Spam
- Spyware
- IM Content Control
- URL Filtering
- Data Loss Prevention
- Anti-Virus

Content

- Biometrics
- Two Factor Authentication
- Single Sign On
- Identity Provisioning

Identity

- Compliance Monitoring
- Security Event/Incident Management

Security Program

- Firewall
- VPN
- Integrated Appliances
- SSL VPN
- Intrusion Prevention
- Wireless

Network

- Application Firewalls
- Email Encryption

Application

- Database Encryption
- Patch Management
- Endpoint Security
- File Encryption
- Media/Tape Encryption
- Storage Encryption

Host

Security Vendor Framework

Information Security Governance Compliance Requirements	**Content**	Data Generated or Requested by a User
	Host	Endpoint Assets: Desktops, Servers, Storage, Handhelds
	Application	Programs/Access for employees, partners, and customers
	Identity	User Provisioning, Access, and Control
	Network	Infrastructure Protection
	Security Program	Reporting, Compliance, Audit and Enforcement of Policy

Point to Ponder

“Intelligence is the ability to adapt to change.”

Stephen Hawking

Current VoIP Attacks

- HTTP Skype
- MGCP Long Endpoint
- NetMeeting Directory Traversal
- H225 Invalid Field DoS
- CiscoSccp Invalid MessageID
- MGCP Long Tid
- H225 Invalid Length DoS
- Cisco H23 Overflow
- H323 Detected
- SIP Long Header Name
- H225 Signaling Message
- SIP Large Content Length
- Protos H225 Attack Tool
- H225 Suspicious Field Length
- SIP Blank Header Value
- SIP Long Method Name
- SIP Unknown Method Name
- MGCP LongField
- STUN Message
- STUN KPhone DoS
- Cisco Sccp Message Underflow
- Cisco Open Receive Channel
- Cisco CallMgrDB DoS
- Cisco CallMgrDB Bo
- SIP Content Length Mismatch
- SIP Large Max Forwards
- HTTP Skye Callto Overflow
- Cisco Start Media Transmission
- Cisco Stop Media Transmission

Security Framework – Best Practices

1. *Maintain Current Patch Levels*
   Inadequate patching exposes risk, unnecessary.

2. *Install Anti-Virus*
   Goes without mentioning

3. *Apply Intrusion Detection/Prevention Systems*
   Current/emerging threats
   Worms, trojans, spyware, etc.
   Call processing environment

4. *Install Application Gateways between trusted/untrusted zones*
   Specific read/interpret/act
   Monitor legitimate/bogus call set ups.
   H.323/MGCP call registration
   SIP – media stream, dynamic assigned port changing per call

Security Framework – Best Practices

5. Enforce SIP security by AAA and IPSec

Monitoring/Spoofing/Registration Hijacking

AAA and IPSec/VPN

6. Establish Policy Based Security Zones

Isolate call processing

7. VoIP over VPN

Reduce chances of eavesdropping in un-trusted portions of network.

8. Use VLAN's to prioritize and protect voice from data network attacks.

Prevent and prioritize

Security Framework – Best Practices

9. Apply encryption selectively

Consider encrypting signaling and/or media streams.
Use selectively, not as broad policy.
Performance?

10. Protect against UDP flooding

Enable UDP flood protection (firewall) feature.

11. Develop holistic security policy

Documentation of security policies and procedures.
Monitor computing resources constantly.
Disable unneeded services on all VoIP components.

Point to Ponder

"Before I came here I was confused about this subject. Having listened to your lecture I am still confused, but on a higher level."

Enrico Fermi

IPCOMM2006

September 25-27 • Gaylord Opryland • Nashville, TN

QUESTIONS?

Contact:

Paul Adamonis
Director, Security Solutions
padamonis@forsythe.com
847-213-7360

FORSYTHE

Delivering the business value of IT℠