Protecting Information in a Changing World

ATP - Columbus

February 8, 2006

Bob West

Agenda

- Introductions
- Current State of Affairs
- 2006 Challenges
- Regulatory Climate
- Impact on Voice and Data
- Approach For Protecting Information
- Keys For Long-term Success

Introductions

- Echelon One - Information security research company founded in March 2005
- Group is comprised of former CISOs, CSOs, Gartner and META Group research professionals
- Differentiators - Experience and focus on security

Current State of Affairs

- Organizational ecosystem is fragile and continues to evolve
- Identity theft hits the headlines
- Systems compromise motive changes from gaining notoriety to gaining profit
- Regulatory acceleration and harmonization
- Product liability for information security problems still a ways off

2006 Challenges

- Spear-phishing
- Extortion
- Corporate espionage
- VOIP, wireless security
- Handheld devices
- Offshore resources, IP and terrorism
- US - FFIEC Guidance
- Annual shareholder meeting
- The landscape continues to change

2006 Challenges

Intellectual Property

"…China presents unique challenges. The central government has long viewed intellectual property not as an individual right, but as something to benefit the state. It encouraged borrowing, if not stealing, technology (especially foreign technology) on which to build a strong economy…"

A Piracy Culture - Beijing continues to defy U.S. and European efforts to stop IP theft
Newsweek International Edition, January 16, 2006

2006 Challenges

Phishing

"More Sophisticated Trojans and Infection Methods Malicious code designed for keylogging consumer data, such as user names and passwords, continues to grow at a rapid and alarming pace. In November, Websense Security Labs™ saw several cases in which commercial websites were compromised and exploit code was placed on them to infect users with Trojan Horse keyloggers upon connecting to the site. The keyloggers usually monitor a consumer's web surfing behavior and capture keystrokes upon visiting popular online institutions."

Phishing Activity Trends Report November, 2005
Anti-Phishing Working Group

2006 Challenges

Spear-phishing

"Arriving home from a five-week trip to Belgium and India on Aug. 14, a jet-lagged Korukonda L. Murty picked up his mail -- and got the shock of his life. Two monthly statements from online brokerage E*Trade Financial (ET) showed that securities worth $174,000 -- the bulk of his and his wife's savings -- had vanished…"

Invasion of the Stock Hackers, BusinessWeek
November 3, 2005

2006 Challenges

Terrorism

"…A suspected militant raid on one of India's top science universities has confirmed fears that the country's booming information technology sector could be a new target for terror groups, officials and analysts said…"

"the use of a Kalashnikov rifle to open fire randomly and the recovery of unexploded grenades and cartridges from the site--points to anti-Indian Islamist militant groups, they said."Whatever information is coming out of Bangalore shows that one of these groups is responsible," said B. Raman, a former head of the Research and Analysis Wing, India's external intelligence agency."Although the damage was not much, it was a very daring attack. Unless there is evidence to the contrary, I would believe this is the work of jihadi groups," he said, referring to Muslim militants fighting Indian rule in disputed Kashmir."

Terror shadow stalks 'India's Silicon Valley'
Reuters, January 2, 2006

2006 Challenges

Extortion

“The e-mail began, "Your site is under attack," and it gave Mickey Richardson two choices: "You can send us $40K by Western Union [and] your site will be protected not just this weekend but for the next 12 months," or, "If you choose not to pay...you will be under attack each weekend for the next 20 weeks, or until you close your doors.”…”

ONLINE EXTORTION- How a Bookmaker and a Whiz Kid Took On an Extortionist and Won, *CSO* Magazine May 2005

Regulatory Climate

- US - Sarbanes-Oxley, SB 1386, GLBA, HIPAA, Patriot Act state laws and pending legislation
- EU - Privacy Directives
- Asia-Pacific - Privacy legislation in Japan
- China and India - concept of intellectual property is foreign and difficult to enforce laws
- Corporate espionage is executed in collaboration with governments
- Developing World - Government interference creates challenging environment

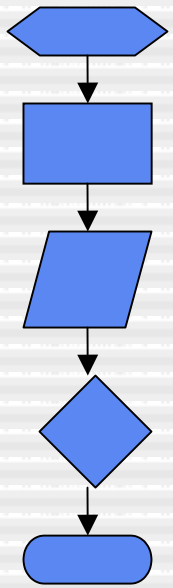
Impact on Voice and Data Networks

- Unprotected systems could be a significant issue
  - Disruption in voice or data impacts business directly
  - VOIP very young, voice now susceptible to IP vulnerabilities and eavesdropping
  - Intellectual property theft
  - Customer information (privacy)
  - Denial of Service Attacks
  - Execution or redirection of financial transactions
  - Extortion
- These issues could impact global economic markets, corporate reputation and image

Approach for Protecting Information

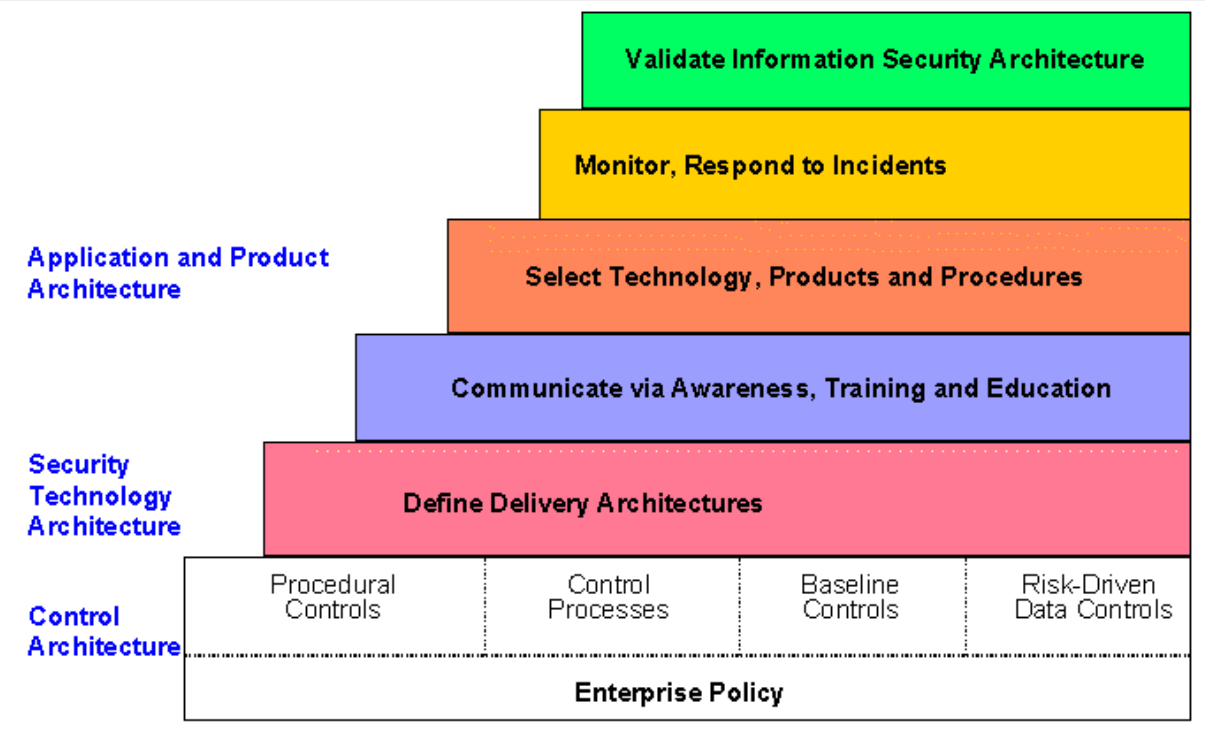
People

Process



Tools

Information Security Hierarchy of Needs

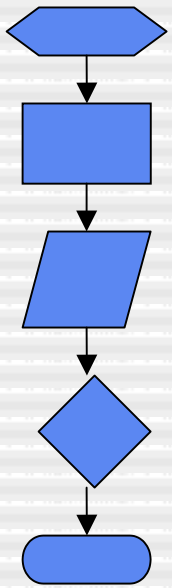


Source: Gartner

Process

Governance

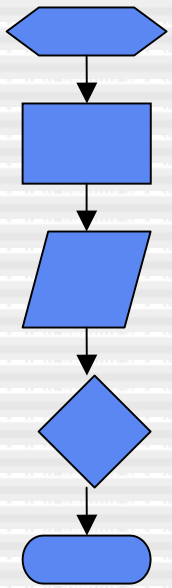
- “Can you, the members of the board of directors, assure us, the shareholders, that our information security policies are being applied fairly and legally in every jurisdiction in which we operate?”
- Alignment with business objectives



Process

Policies and Standards

- Policies must be simple, direct, teachable, trainable. Biggest return on investment of any security initiative
- Simple test: An employee sees someone doing something that might be wrong – ask three questions:
  1. Would she know if it were wrong?
  2. Would she choose to report it?
  3. Would she know whom to call?



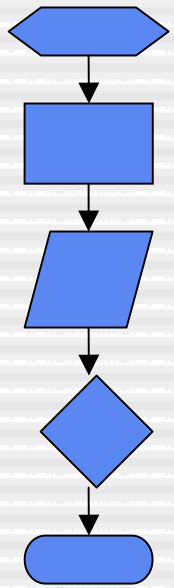
People

- Communication
  - Internal
  - External
- Awareness and Education
  - Executives
  - Employees and business partners
  - System administrators
  - Application developers
  - Project Managers

Process

Architecture

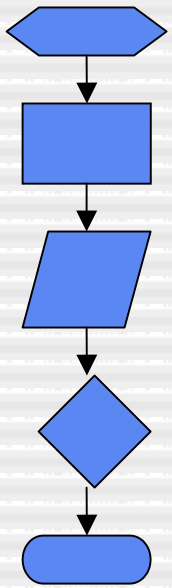
- Not a technology issue! It's a business architecture issue –
  - Define a set of architectural primitives like "access control", "confidentiality"
  - Break down policy and governance directives
  - Map each directive to its set of functions
  - For each platform identify criteria governing tool, selection



Process

Incident Response

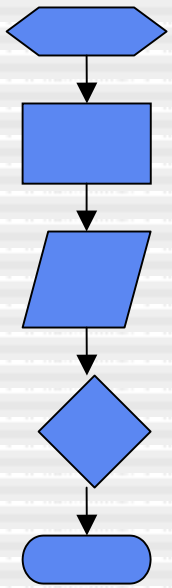
- Need to have pre-defined process and the right people across the corporation engaged
- Don’t reinvent the wheel
- Script for communication to the media is often overlooked



Process

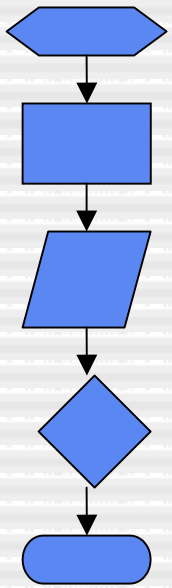
Application Development

- Integration into development process
- Developers need to be educated
- SDLC marries SEI CMM
- If you can specify a security metric, then you can test for it; if you can't, you won't



Process

- Business Continuity
  - How does business continue with minimal interruption during natural disasters and terrorist attacks?
- Disaster Recovery
  - Disasters come in pairs – going to other site and then coming back
  - Use the DR plan for normal data center moves
  - Desk check the plan, test when feasible



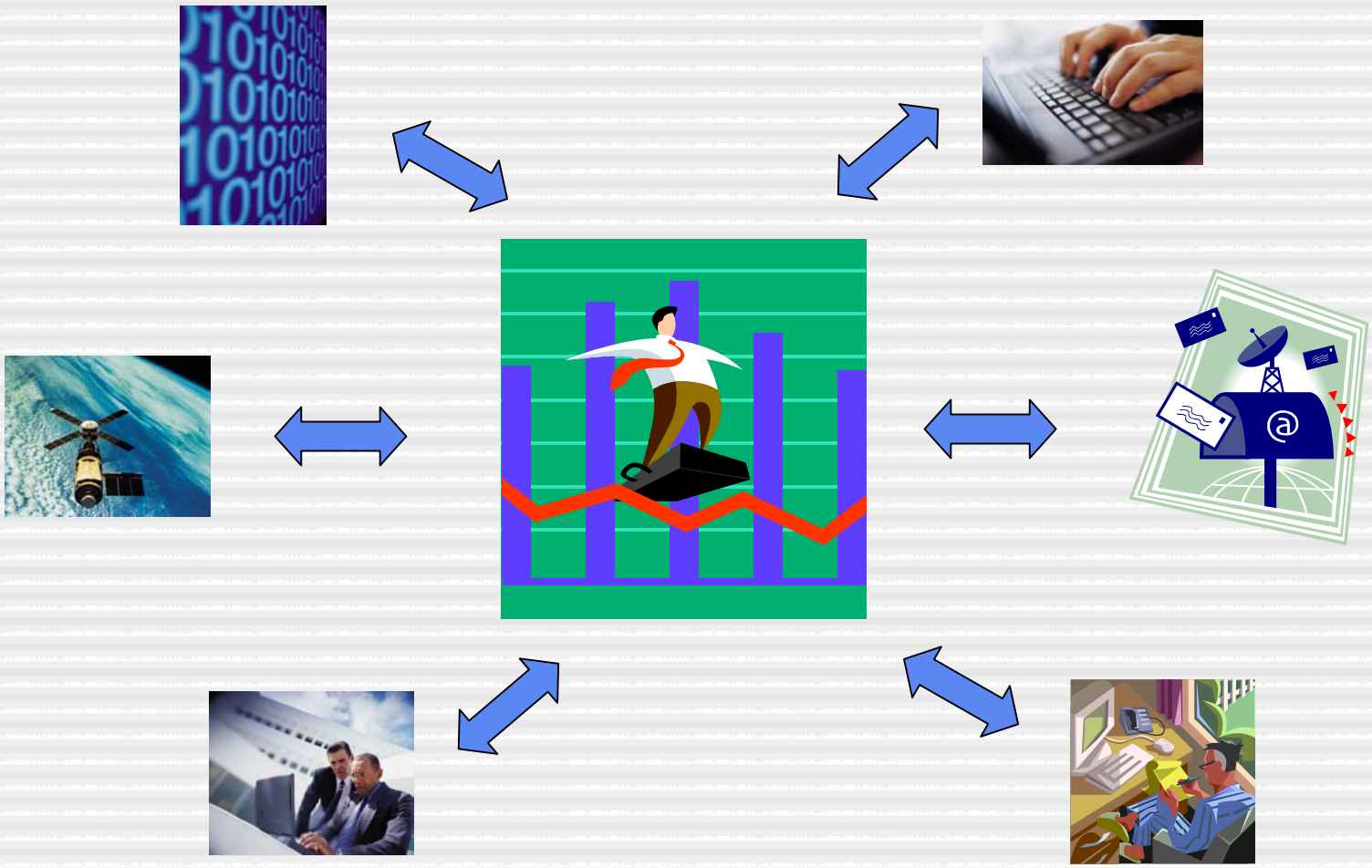
Tools

- Firewalls
- Vulnerability Management
- IDS/IPS
- Anti-virus
- Spyware
- Authentication
- Encryption
- Application Security

Keys for Long-term Success

- Global enterprise and industry focus
- Manage relationships
- Business alignment
- Monitor emerging issues and changes in both technology and geography; scenario planning pays dividends
- Review plans regularly and modify as necessary
- Communicate, communicate, communicate
- People, process, tools

Achieving a Balance



Q&A

Thank You!

Bob West
bob.west@echelonone.net
513-328-7430