

# **It's a People Problem, not a Technology Problem**

Daniel Rothman  
February 7, 2006

# The Seas of Information

- Connected Water
- Touches Everyone
- Jump In, the Water's Fine!



# Dangerous Waters

- The Open Internet
- Breakwaters
  - DMZs
  - Extranets



# The Safe End of the Pool

- Finance/Accounting
- Personnel
- Data Warehouse
- Decision Support



# Off the Deep End

- Cubicles and Desktops
  - Office Productivity
  - Email
  - Internet Browsing
- Road Warriors
  - Sales Applications
  - Catalog Applications
  - Remote Connectivity
- Wireless
- PDAs



The Florida Times-Union / Jon M. Fletcher

# Disease

- Viruses
- Malware
- Spyware



# Pollution

- Leakage
  - Personal Information
  - Customer Information
- Misinformation
- Hate Speech
- Pornography



# Sharks in the Waters

- Phishing E-mails
- Viruses
- Hacking
- Social Engineering
- Dumpster Diving

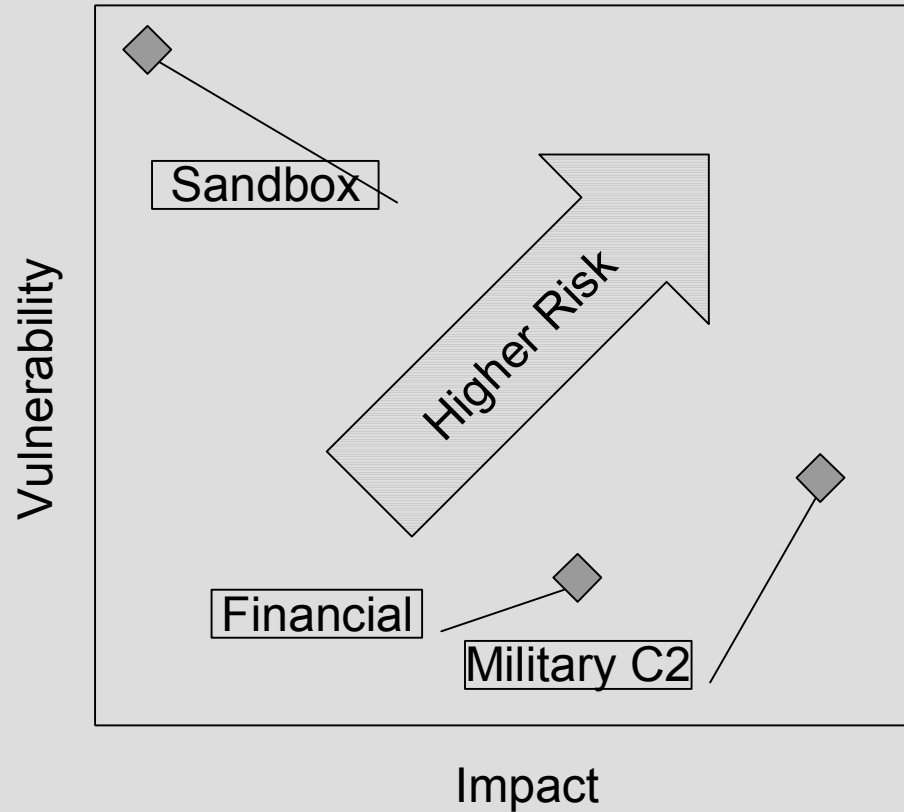


# Total Risk

- Vulnerability
  - Threat
  - Exposure
- Impact
  - Data Loss
  - Monetary Loss
  - Loss of Life
- Mitigations
  - Total Risk is mitigated in these two areas
  - Reducing Vulnerability
    - Reduced exposure
  - Reducing Impact
    - Tighter controls for greater impact transactions
    - Isolating functions to reduce “collateral damage”

# Range of Risks

- Laboratory “Sandbox”
  - Controlled exposure
- Financial Reporting System
  - Controlled vulnerability
- Military Command and Control
  - Closely controlled vulnerability
  - High Impact



# Threats are Not What They Used to Be

## Something Old

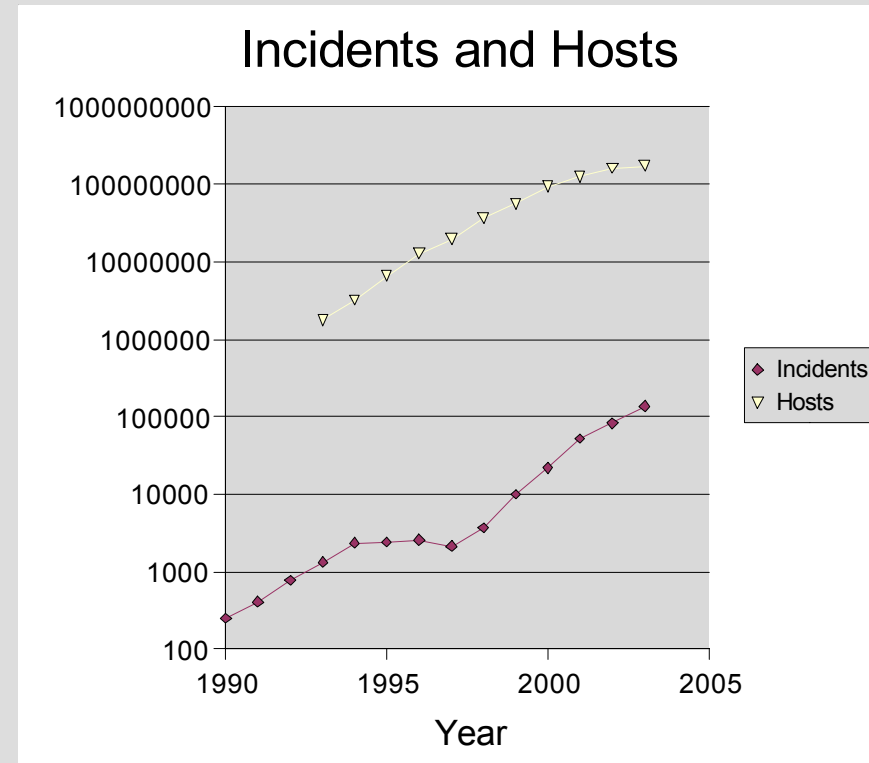
- Virus, Spam, Phishing
- Downtime
- Teenage Hacker
- Remote Access
- National Problem
- Malign Insider

## Something New

- Blended Threat
- Zombie Network
  - Distributed Denial of Service
- Professional Attacks
  - Foreign Military
  - Organized Crime
- Roaming, Wireless
- Globalized Issue
- Maladroit Insider

# Accelerating Threats

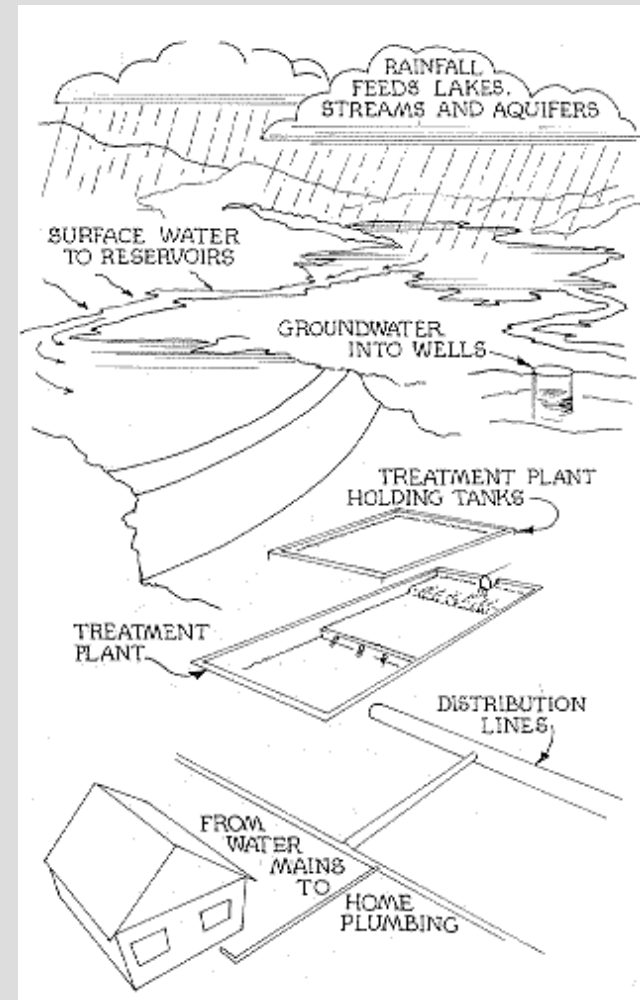
- CERT (at CMU) Incident Response Reporting
  - Not reported after 2003
- Incident reports growing faster than Internet



“Given the widespread use of automated attack tools, attacks against Internet-connected systems have become so commonplace that counts of the number of incidents reported provide little information with regard to assessing the scope and impact of attacks. Therefore, as of 2004, we will no longer publish the number of incidents reported. Instead, we will be working with others in the community to develop and report on more meaningful metrics.” Carnegie-Mellon CERT/Software Engineering Institute

# Our Interconnectedness

- Like our water supply, we're all linked by the seas of information
- Approaches to assurance must change
  - Old: “barbarians at the gate” perimeter defense
  - New: “public health” monitoring, preservation, filtration – grass roots



# Business Impacts

- Downtime
  - Russian Stock Market Offline Friday
- Financial Losses
- Data Leakage
- Compliance
  - Sarbanes-Oxley
  - HIPAA
- IT Budgets
  - Hardware, 5%-10%
  - Software, 10%-30%
- Top of CIO Priority Lists for 2005

"Klez, about \$9.5 billion; Love Bug, about \$9 billion; Code Red, \$2 billion; Slammer, \$1 billion; Sobig.F and Blaster combined, somewhere in the neighborhood of \$3.5 billion." Kenneth Silva, Verisign, testimony before House of Representatives, Subcommittee on Telecommunications and the Internet, Washington, DC, 11/2002

# Mitigation

- Security Best Practices
  - reduce TCO indirect costs due to downtime by 40% - 55%.
  - reduce overall TCO by 14% - 17%

Security Best Practices Can Lower PC TCO, Gartner 12/2005

- ***“Insider incidents were detected by a range of people (both internal to the organization and external), not just by security staff. Both manual and automated procedures played a role in detection.”***

*Insider Threat: Real Data on a Real Problem, Dawn Cappelli, Michelle Keeney, 11/2004*

# It's the People, not the Technology

- Your Strongest Asset
  - Your people accomplish your mission
  - Use the boots on the ground
- Your Weakest Link
  - Every employee is a potential threat vector
  - Proactively reduce your risks
- Empower the Workforce
  - Recognize and resist social engineering
  - Develop a culture of good information security hygiene

"no technology in the world can protect an organization if users exercise bad E-mail behavior", User Ignorance To Blame For Spam, Information Week 3/2005

# Broad Spectrum “Cocktail”

- DoD Applies DOTMLPF Analysis
  - Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, and Facilities
- Current Industry Practices Center on Materiel
  - Not well balanced and leveraged with other elements of a broad spectrum solution
- Training, Leadership, and Personnel
  - Where applied in standard practice, are focused on IT Department

# Specific Strategies

- Doctrine
  - Policy and Procedure
    - Acceptable Use
    - Data Protection
- Organization
  - Not Just IT
    - Engage and Commit all Board of Directors
- Training
  - Empower All Levels of Enterprise
  - Practical Tips, not Reiteration of Policy
- Materiel
  - Technical Approaches
- Leadership
  - Executive Practices
- Personnel
  - Carrot and Stick
    - Reward and Recognize security contributions from all segments
    - Support Policy with personnel actions
- Facilities

# Policy and Procedure

- Policy

- Tie to practice
- Address to specific audiences
  - Isolate technical for IT implementation and management
  - Avoid technical in operational and administrative
- Tie to personnel
  - Recognition and reward, as well as penalties

- Procedure

- “Rubber Meets the Road”
  - Playbooks for peoples' desktops
  - As ubiquitous and usable as corporate powerpoint templates
- Keeps up with Tech
  - Each System, Each Version
- Keeps up with Org Chart
  - Who to call for guidance

# Organization

- **Different Tribes, Different Cultures**
  - Information Technology (CIO)
  - Sales (CSO/EVP Sales)
  - Executive Management (CEO)
  - Back Office/Administrative (CFO)
  - Product/Marketing (CMO/EVP Marketing)
  - Operations/Manufacturing (CTO/COO)
- **Different Total Risk**
  - Different exposures and vulnerabilities
  - Different impacts
  - Applying DOTMLPF for best value (bang for the buck) w should employ targeted strategies for total risk mitigation
- **Total Risk for the Total Enterprise**

# Training

- Who
  - Everyone
  - All the “tribes”
  - Appropriate content and delivery
  - **Executives too!**
- How
  - Concrete methods
  - Practices and behaviors
  - It's Not The Technology!
- When
  - In-Processing
  - Short, sharp, recurring refresh
    - Paced with changes in best practices
- Why
  - Develop Culture
    - Instill in the grass roots
    - Lead from the top
  - Ubiquitous Practices
  - Adaptable to Change

# Train - What?

- Prevention
  - Preserve Information
    - Travel
    - Transport
  - Secure Access
    - Remote Access
    - Wireless
    - Mobile Devices
  - E-mail and Web
    - Resist phishing
    - Avoid sites with malware
  - Resist Social Engineering
- Detection
  - Recognition
    - Physical Security
      - “Where's your badge?”
    - Intrusion attempts
      - Phishing
      - Social engineering
      - Spam
  - Reporting Procedures
    - What information
    - How to report

# Outcomes

- Ubiquitous Internal Monitoring
  - Physical security
  - Network health
  - Attempted intrusions
- Reduced Exposure
  - Greater awareness of information handling
  - Best practices for threat response
- Support and Feedback for Technical Capabilities
  - Reduced “workarounds”
  - Behaviors to complement technology solutions

**A Cleaner Pool for All of Us!**

# We're All in the Same Lifeboat

What goes around  
comes around

