Vulnerability Management in Action

Nebraska CERT Conference 2009
Bill Dixon
Continuum Worldwide

Vulnerability Management

- Vulnerabilities exist in:
  - Software
  - Hardware
  - Facilities
  - People
  - Processes

Risk Management 101

- Risk = Asset x Vulnerability x Threat – Safeguard
- Tracking the vulnerability is a key element in vulnerability management, but what is a vulnerability?

Vulnerability

- a weakness in information system security design, procedures, implementation, or internal controls that could be exploited to gain unauthorized access to information or an information system

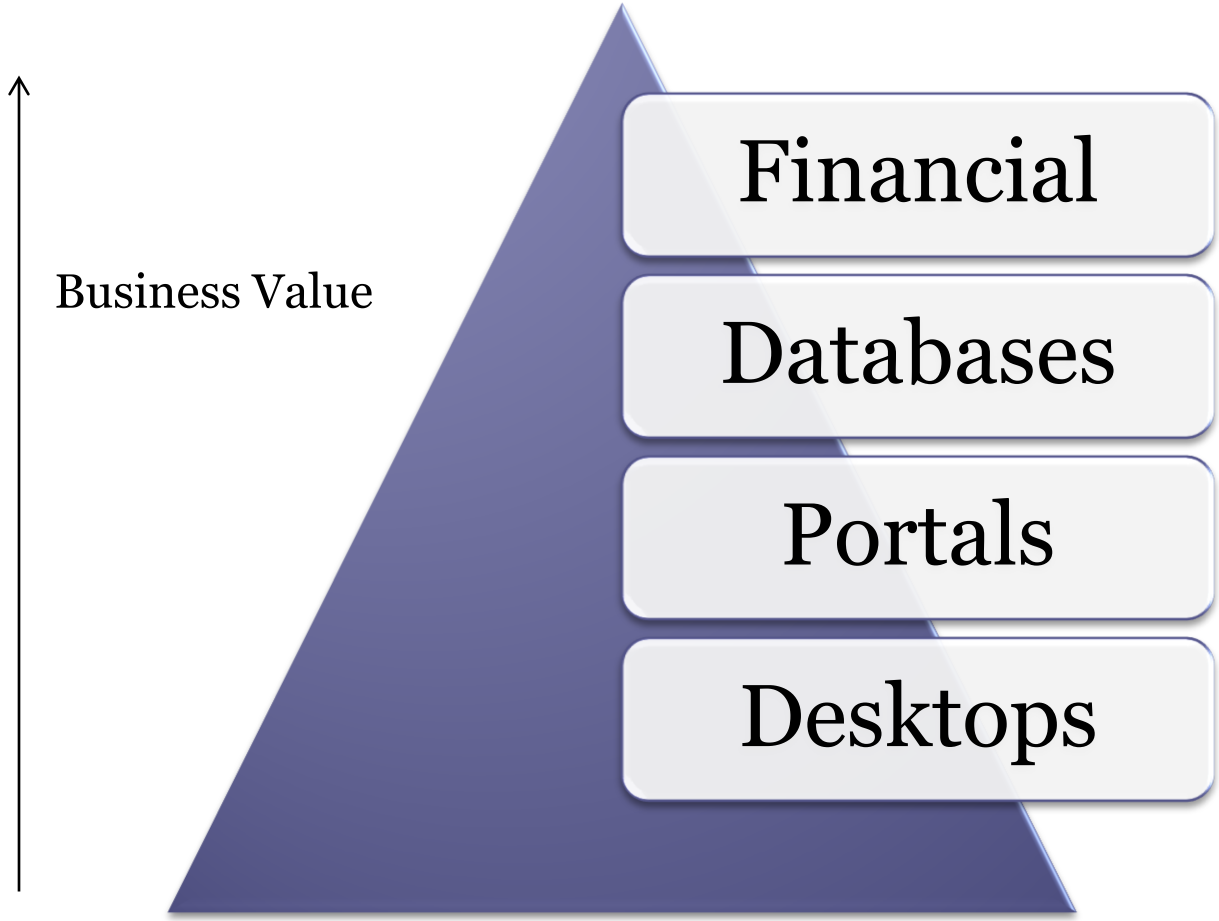
Sources for vulnerability identification

- Vulnerability scanners
- Audits
- Risk assessments
- Vendors
- Incidents

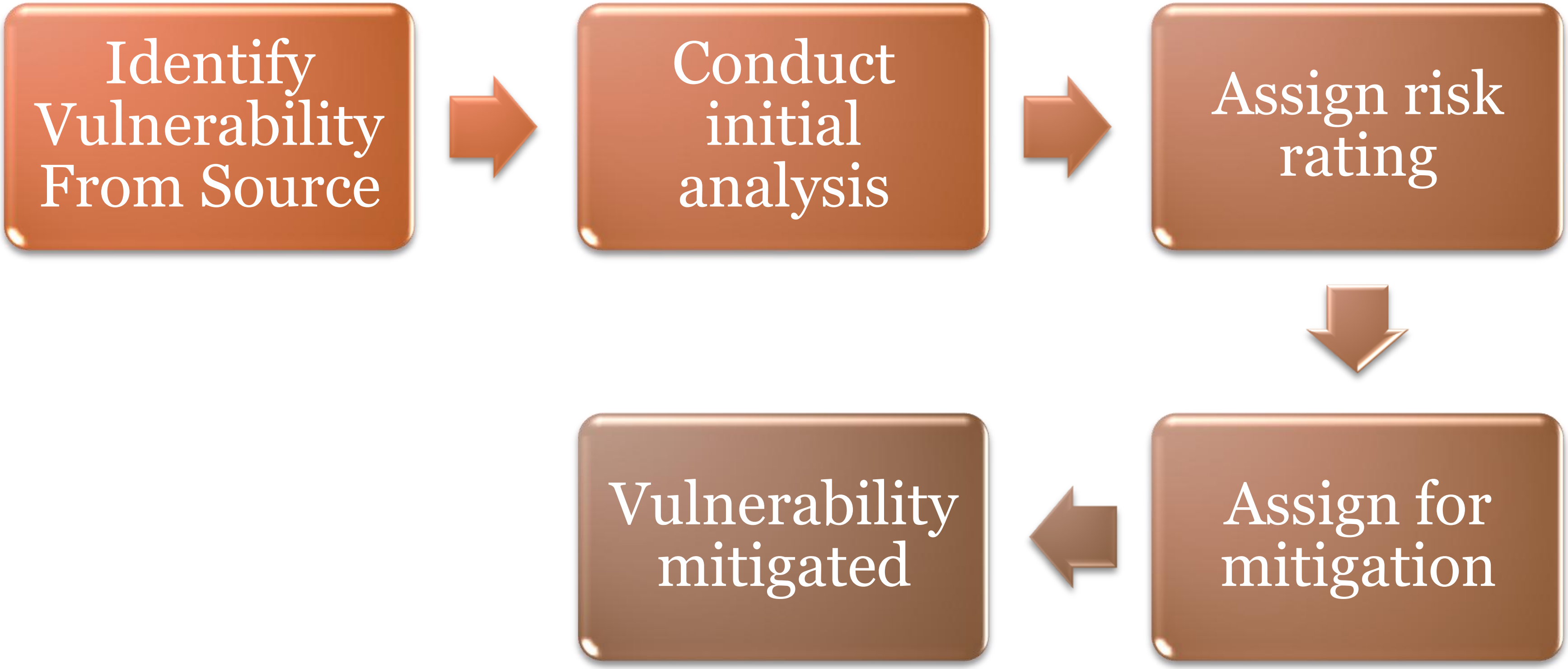
Issues

- Multiple sources – with or without analysis
- Reluctant system administrators
- Hard line security professionals
- Misperception of value of the asset

System Business Value circa 2003

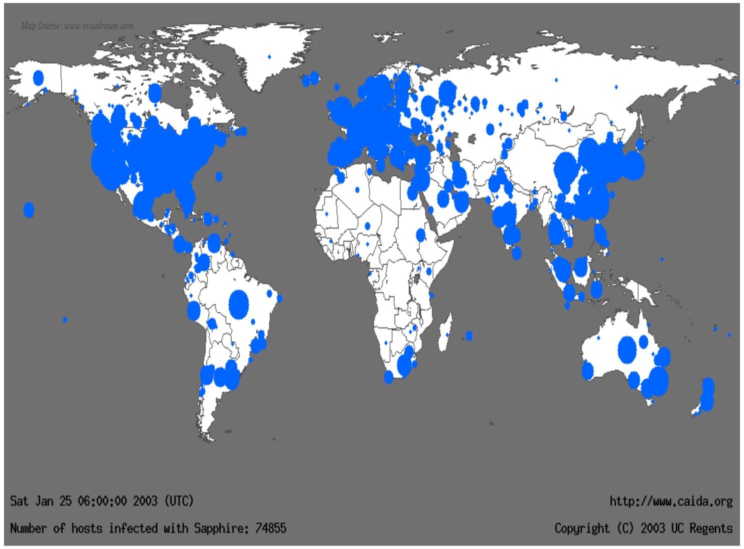


Vulnerability Management Cycle



What action is taken?

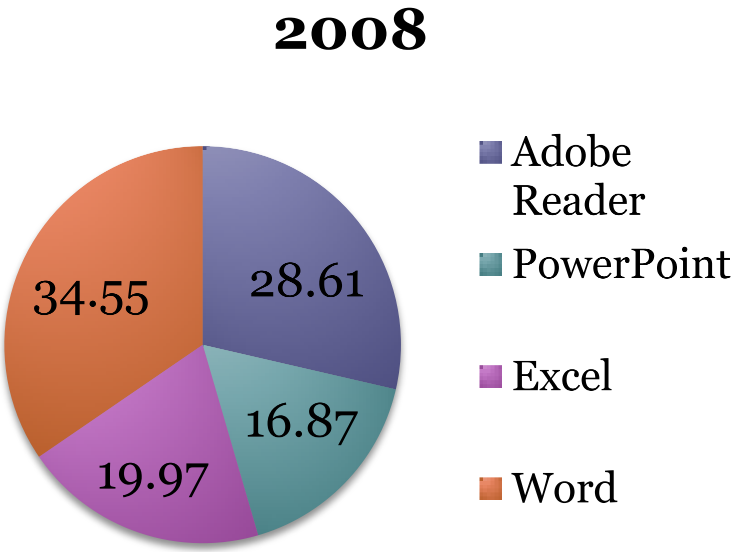
- Address those vulnerabilities that are perceived to have the biggest threat to the organization.
- Threats to critical components
  - DMZ – customer facing systems
  - Systems that house data
- 2003 – SQL Slammer Worm

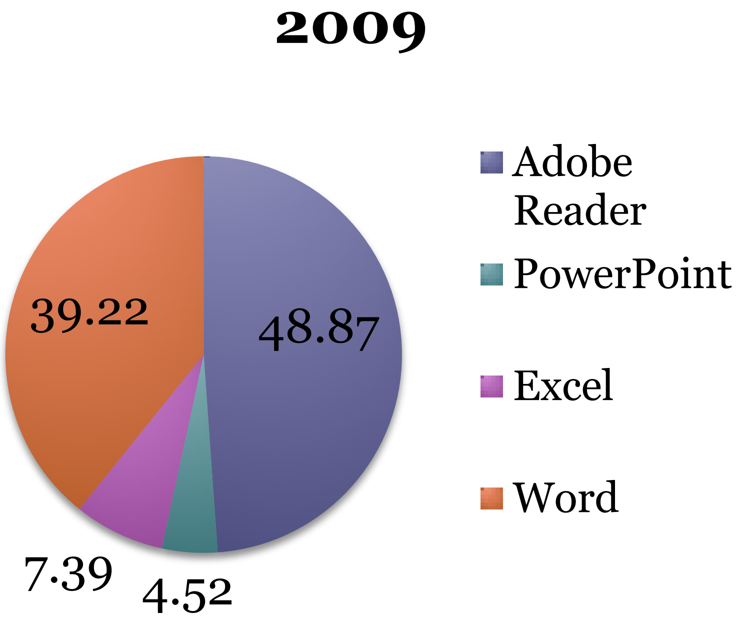

Map Source : www.visualroute.com
Sat Jan 25 06:00:00 2003 (UTC)
http://www.caida.org
Number of hosts infected with Sapphire: 74855
Copyright (C) 2003 UC Regents

What has changed?

- The landscape of the attack vector
  - Application focused
    - Web applications
    - End user applications
- Low hanging fruit for attackers
- The “core” has been protected from the outside in

Common attack targets



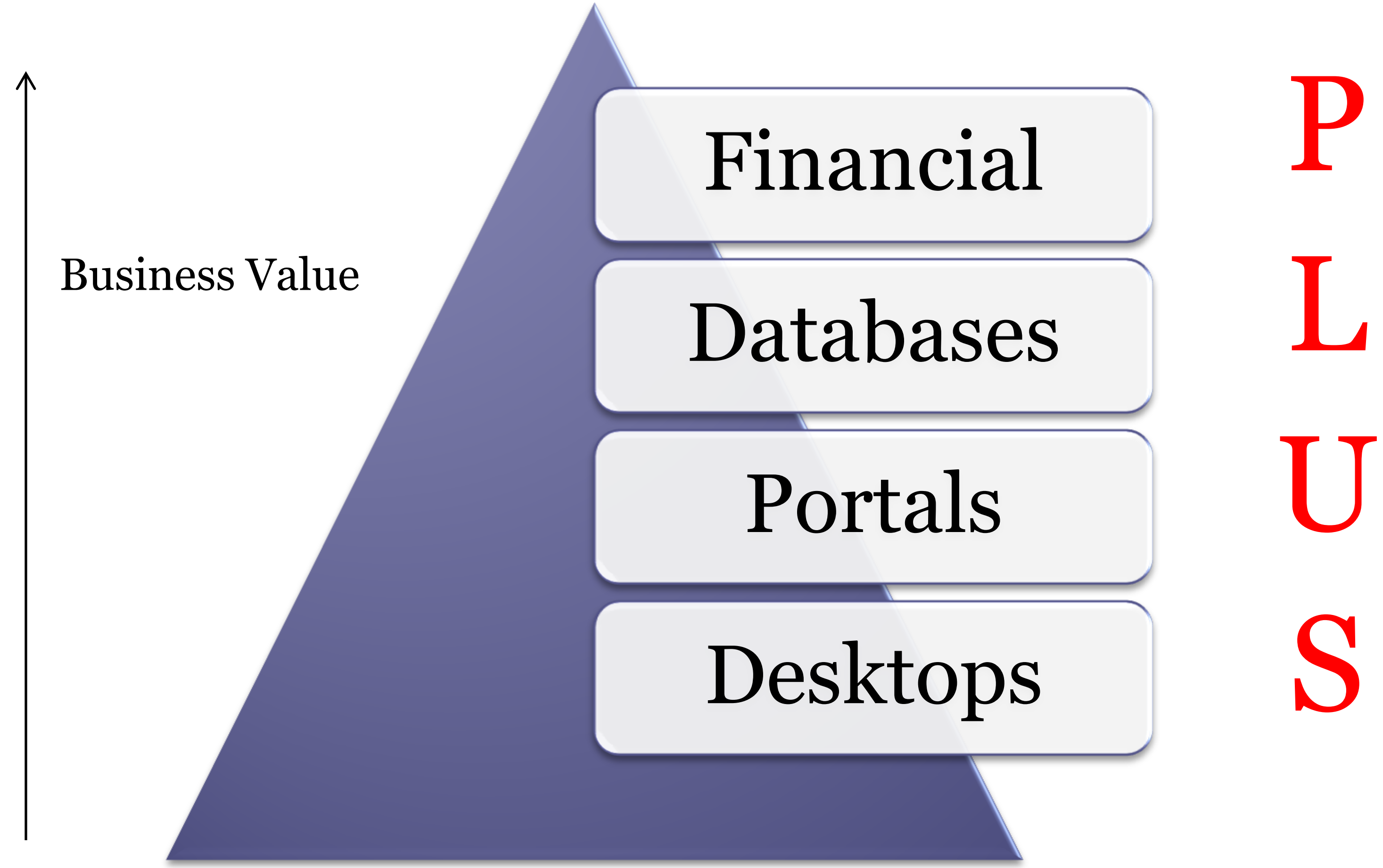


Source: 2009 *The Laws of Vulnerability Management 2.0, Qualys Inc.*

Evidence of shift

- 2008
  - RBS Worldpay
  - Hannaford Foods
- 2009
  - Heartland Payment Systems
- Common theme:
  - Client based attack vectors

System Business Value circa 2009



New factor for action

- Client systems
  - What do they have access to?
  - Who uses the system?
  - What is really stored on the client?

Challenges in Vulnerability Management - 2009

- When adding the dynamics of client systems
  - Versioning of software loaded
  - OS loads, configurations
  - Monitoring
    - Sampling… maybe not
    - Priority bases… maybe, but other controls may need to be in place

What about 0 days?

- Good patch management still applies
- Run a modern OS
- Baseline security configuration standards
  - OS
  - Applications
- Asset identification
- Awareness

Vulnerability Management Today

- Proactive approach
- Expanded and integrate identification sources
  - Not just watching for patches
  - Sources
    - Audits
    - Penetration Tests
    - Incidents

Bridging the Vulnerability Gap

- Action
  - Day to day management
  - Increase awareness
  - Look at systems
    - What is accessed – This applies outside of the enterprise
  - Analyze the scenario
    - Likelihood
    - Impact
    - Resource appropriately

Questions

Bill Dixon, CISSP, CISM

Bill.dixon@continuumww.com