THE CASE FOR PROACTIVE NETWORK SECURITY: WORMS, VIRUSES & BUSINESS CONTINUITY

Presented to Dr. Yan Chen
MITP 458- Information Security & Assurance
Business Case Study Presentation
09 June 2007
by *The Loop Group*
Farney, Heilprin, Leonard

2001: THE END OF REACTIVE NETWORK SECURITY

The Year of the Worm; (3) major worms released July-September 2001

- **Code Red**
  - **$2.6bn estimated damage**
  - **Simple buffer overflow infected 350,000+ hosts in single day**
- **Code Red II**
  - **Same attack vector (.ida), but different signature**
- **Nimda**
  - **Mass-mailing, multivariate attack**
- **All based on previously released and patched vulnerabilities**
  - **MS01-033, MS00-052, MS00-078, MS01-020**
  - **A/V software useless**
- **Used firewall ports not needed (externally) in the first place**
  - **135, 137, 138, 139, 445, 593, 1639, 2000-3000, 3127-3198**

100% Preventability!

"HEROIC IT" NOT ENOUGH, PEOPLE *AND* PROCESS REQUIRED

Speed of attack dispersion and increased geographic expansion make it impossible to react to today's threats

- **Design and deploy network security operations infrastructure in which automatic patch management plays central role**
  - **Vulnerabilities addressed on release day (making test assumption)**
- **Proactively tighten defenses**
  - **"deny all" vs. "allow all" on interior firewall interfaces**
  - **Perform network analysis to determine required business functions and corresponding ports, deny all else**

2001 attacks responsible for major shift in corporate defenses

(1) *Heroic IT Management Is No Longer Enough*, Diamond Cluster Viewpoint, 2004