

# Security Challenges and Solutions

## John Porter

- I. Mitigating Vulnerabilities
  - Create an internal IT Security Officer position
  - Conduct security audits and annual financial systems audits by external auditors
  - Conduct business impact assessment by external assessors
  - Conduct periodic internal system and security audits
- II. Security Plan Development
  - Develop plan from perimeter to core network
  - Security model based on industry research, Gardner, and federal government guidelines
- III. MCPS Security Model
  - Email viruses, WORMS, malicious code – McAfee Group Shield (Exchange), Web Shield (FirstClass)
  - Desktop anti-virus protection – McAfee Anti-virus (WORMS and Trojans)
  - Email SPAM and denial of service – IronMail (email firewall)
  - Hackers – Cisco PIX firewall, Real Secure intrusion detection
  - CIPA compliance – BESS N2H2
  - Disaster Recovery – fireproof vault, Iron Mountain offsite storage, Sungard Disaster Recovery (hot site)
  - Security alert services - SANS Institute, CERT, XForce, NT Bug Trak, Microsoft, Cisco
  - Security awareness training – staff and students
  - Policies, regulations, procedures
- IV. Lessons Learned
  - Have a plan to survive computer virus attacks
  - Security awareness is most important in preventing security issues
  - Frequent review of perimeter security and system security configuration reduces security events

Produced by:

