CONFERENCE PROGRAM & PROCEEDINGS MATERIAL

For 23rd National Information Systems Security Conference

Title of Presentation: **Guerilla Security: The Martial Art of Infoscurity**

Speaker:

Andrew T. Robinson
President
net/main infoSecurity Solutions

Presentation Topics:

1. Active versus passive information security strategies
2. RAPID[tm] methodology for designing and maintaining an information security plan which is relevant, adaptable, and continuously validated
3. Use of penetration testing to validate your information security plan
4. Incident response and forensic analysis
5. Case study for information securty deployment

Speaker Biography:

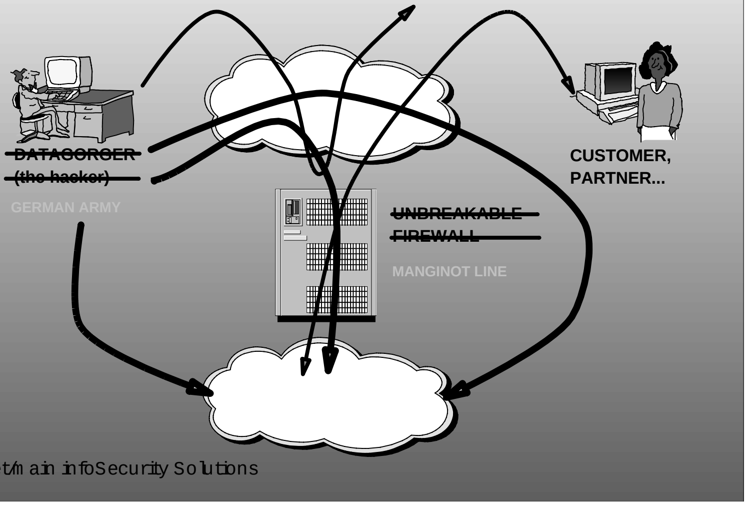
Mr. Robinson has over fifteen years of experience as an Internet security analyst, software engineer and systems integrator. In August 1990, he started net/main infoSecurity Solutions, providing Internet security, integration, and software engineering services on a consulting basis to customers throughout the United States. Mr. Robinson speaks on information security topics at several national conferences each year.

GUERILLA SECURITY

The Martial Art of Infosecurity

PART I: RAPID

Lessons (not) Learned

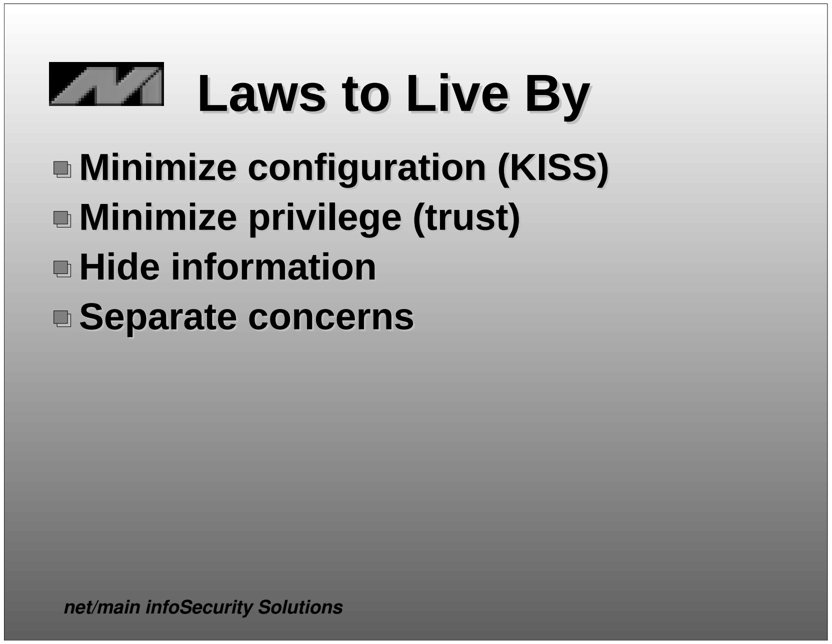


Firewall Follies

- Traditional firewall is a static defense
- Large software system, subject to bugs
- Firewall passes protocols without analysis
- May not protect against...
- Inside jobs
- Parasitic software
- Dialups & dedicated links
- Social engineering

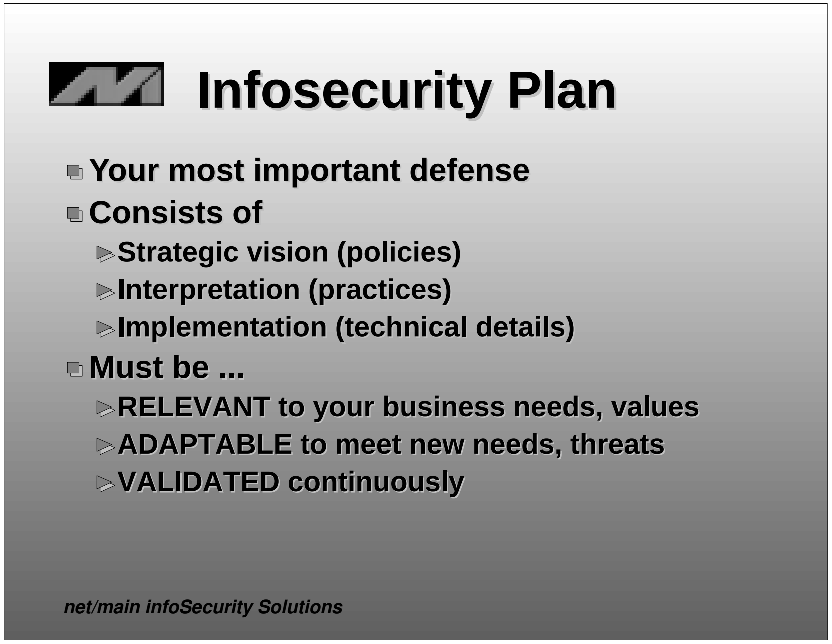
Shoot Your Firewall?

- No!
- Reduces DMZ
- Hides information (and mistakes)
- Concentrates perimeter defenses
- Provides simplified point-of-presence



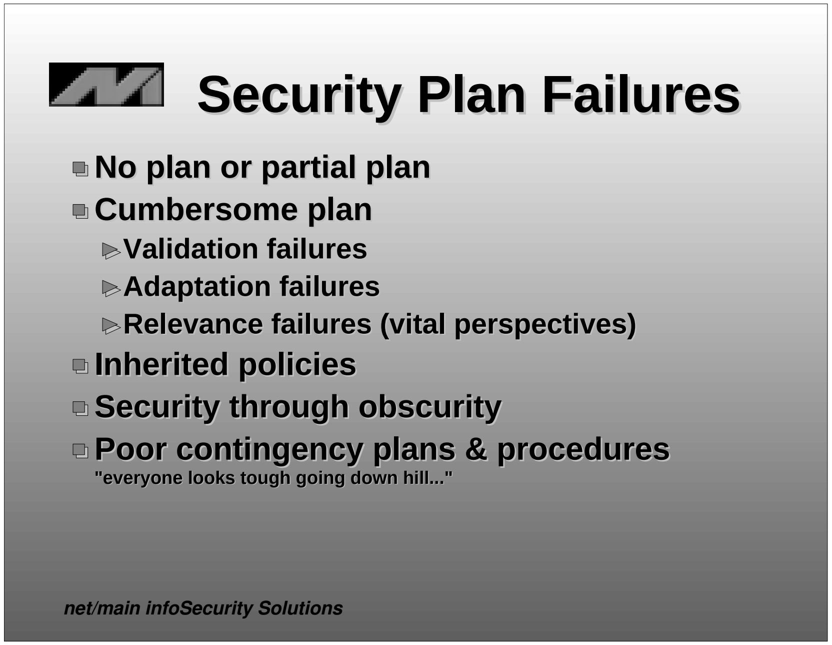
Laws to Live By

- Minimize configuration (KISS)
- Minimize privilege (trust)
- Hide information
- Separate concerns



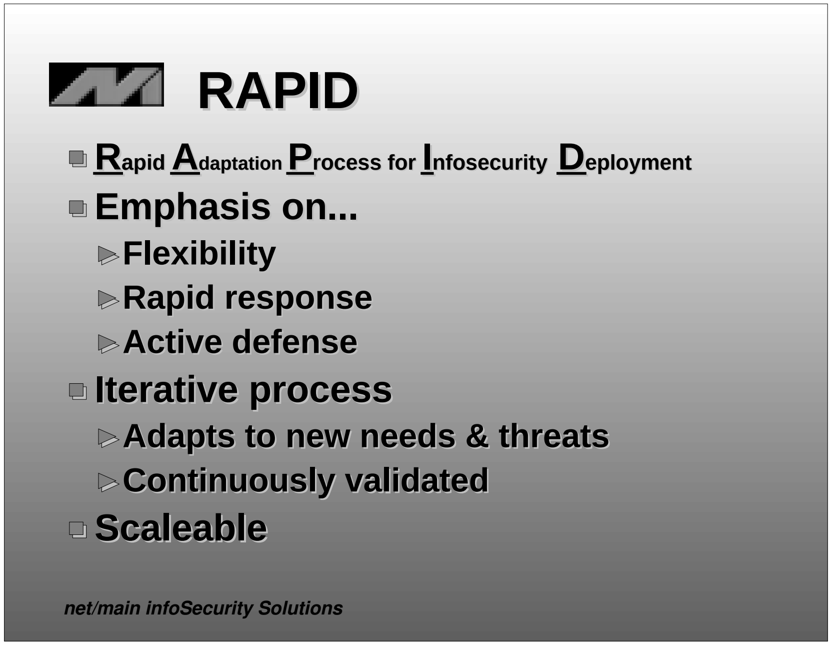
Infosecurity Plan

- Your most important defense
- Consists of
  - Strategic vision (policies)
  - Interpretation (practices)
  - Implementation (technical details)
- Must be ...
  - RELEVANT to your business needs, values
  - ADAPTABLE to meet new needs, threats
  - VALIDATED continuously



Security Plan Failures

- No plan or partial plan
- Cumbersome plan
  - Validation failures
  - Adaptation failures
  - Relevance failures (vital perspectives)
- Inherited policies
- Security through obscurity
- Poor contingency plans & procedures
  "everyone looks tough going down hill..."



RAPID

- Rapid Adaptation Process for Infosecurity Deployment
- Emphasis on...
  - Flexibility
  - Rapid response
  - Active defense
- Iterative process
  - Adapts to new needs & threats
  - Continuously validated
- Scaleable

First Steps

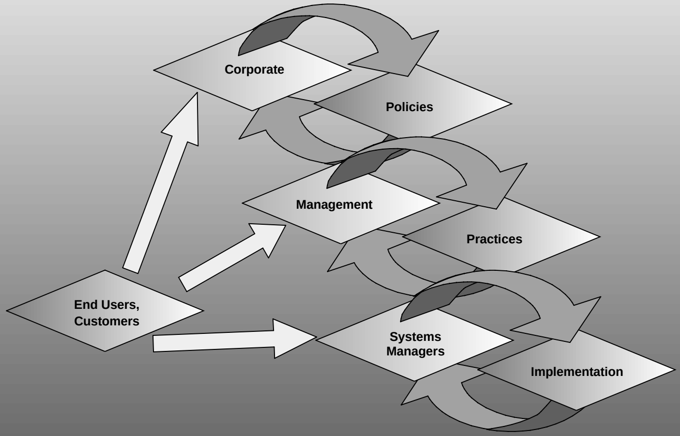
- Identify areas of responsibility (AORs)
- Identify vital perspectives
- Designate security planning (SPT) teams
- Take a Quick Inventory
  - Resources
  - Threats
  - Existing policies & practices
  - Known problems

RAPID Cycle

- Scheduled vs. Triggered

1. Make HIT LIST of important issues
2. Review existing mitigating controls
3. Brainstorm on improvements
4. Update security plan language
5. Publish updates
6. Implement improvements
7. Validate!

RAPID Process



Penetration Testing

- Controlled hacking
- Perspectives
  - Black box -- untrusted outsider (Internet hacker)
  - White box -- trusted insider
  - Gray box -- collaboration between black & white
- Invasive vs. noninvasive
- Single vs. multilevel
  - Don't stop at your firewall (the goodies are mostly behind it)

Case Study

- Financial institution
- Connected to the Internet
- Inside users access WWW, email
- Preparing to go live with eBanking
- Minimal infosecurity planning
- "But we have a firewall!"

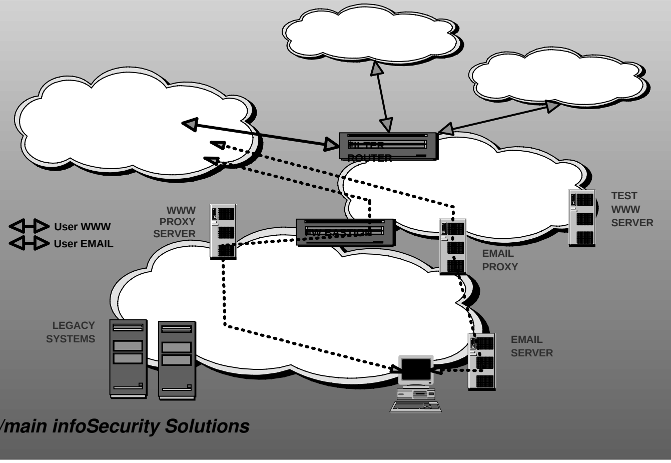
RAPID Kickoff

- Identify two AORs
  - Corporate
  - Systems
- Vital perspectives
- Designate SPTs
  - Corporate SPT to meet quarterly
  - Systems SPT to meet monthly
- First hit list
  - Run PT on Internet/eBanking setup
  - Review existing policies & practices

RAPID Findings

- Company has a security policy
- Policy has not been updated in years
  - Does not reflect Internet threat environment
- Internet implementation uncoordinated
- Known weaknesses in perimeter
- Firewall bypassed for electronic mail
  - Vendor didn't know how to configure FW
- Too many hosts in Internet DMZ
- Extranet connections open to Internet!

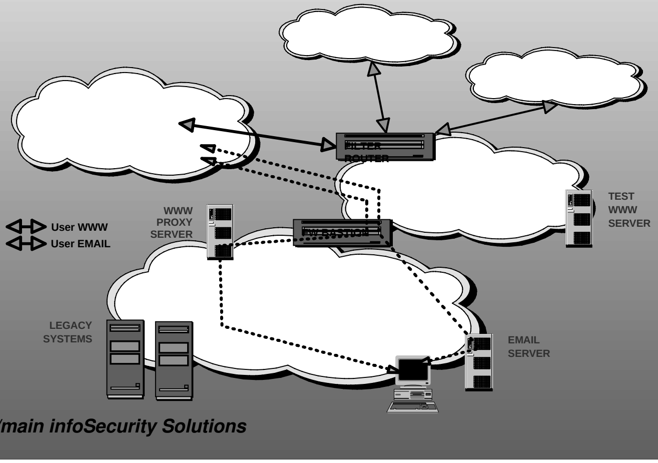
Case Study: Initial Configuration



Initial Penetration Test

- Noninvasive, single level, black box
- Filtering router accessible
- Unpatched NT
- Known denial of service exploits
- Known remote access exploits
- Known confidentiality compromise exploits
- Firewall very strong
- Unnecessary complexity

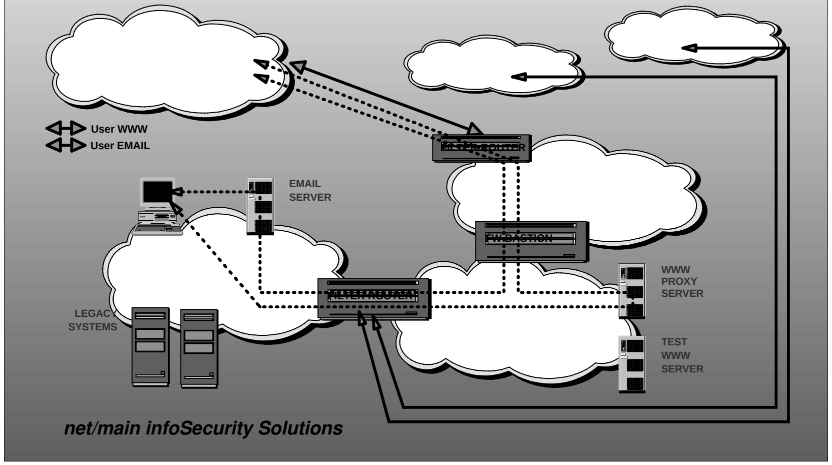
Case Study: Phase I Redesign



Phase I Analysis

- Protect filtering router
- Harden test WWW NT box
- Remove EMAIL proxy NT
- Route EMAIL through firewall
- Harden WWW proxy server

Case Study: Phase II Redesign



Phase II Analysis

- Move extranet out of IDMZ
- Move WWW test to SDMZ
- Isolate service hosts from PNET
- Note analysis of IDMZ only!
- Should test SDMZ, PNET

Case Study Review

- Use of penetration testing
- Application of infosecurity principles
  - Minimal configuration
  - Information hiding
  - Separation of concerns
- Iterative improvement in infosecurity
- Initial state includes many "how not tos"
- Demonstrates RAPID methodology

PART I: THE END

Andrew T. Robinson
net/main infoSecurity Solutions
atr@nmi.net
207-780-6381

Source material for this presentation was taken from the book, *Guerrilla Security* by Robinson et al. *Guerrilla Security* cites many other sources and references.

To obtain a copy of *Guerrilla Security*, please leave your business card with the presenter.

The following are trade or service marks of net/main infoSecurity Solutions:

Guerilla Security
The Martial Art of InfoSecurity
RAPID (Rapid Adaptation Process for InfoSecurity Deployment)