



## Practical and Personal Security

Security Watchdog Enablement  
from the Ideahamster Organization

Copyright 2002 - Pete Herzog

## Practical Security

- Usability
- Cost to Effectiveness
- Limits of Technology
- Assessing and Managing Risk
- Marketing and Competitive Intelligence
- Security Policy
- Securing Processes
- Security Testing

Copyright 2002 - Pete Herzog

## Personal Security

- Privacy
- Safety
- Training / Social Engineering
- Legalities
- Ethics
- Convenience
- Freedom

Copyright 2002 - Pete Herzog

***That is what learning is. You suddenly understand something you've understood all your life, but in a new way.***

***Doris Lessing***

Copyright 2002 - Pete Herzog

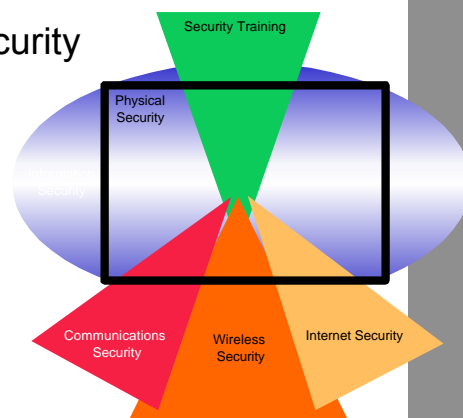
## Security Concepts

- The Great Wall
- The Guarded Doorway
- Encryption and Obfuscation
- Unique Stamps and Signatures
- The DMZ
- The Illusion
- Containment
- Peace
- Aggression
- Disinformation
- Unavailability

Copyright 2002 - Pete Herzog

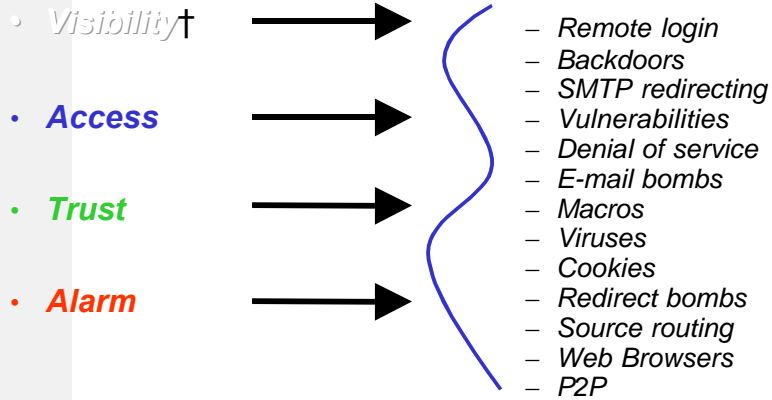
## Security Map

- The security map is a visual display of the security presence
- Communications Security
- Internet Security
- Information Security
- Physical Security
- Wireless Security
- Security Training



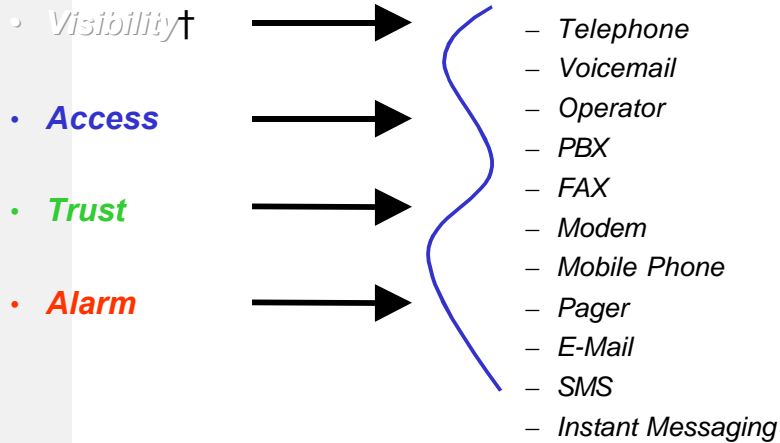
Copyright 2002 - Pete Herzog

## Internet Security Presence



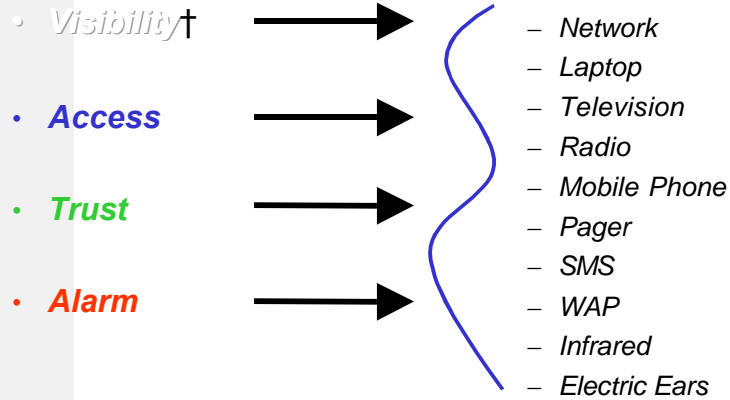
Copyright 2002 - Pete Herzog

## Communications Security Presence



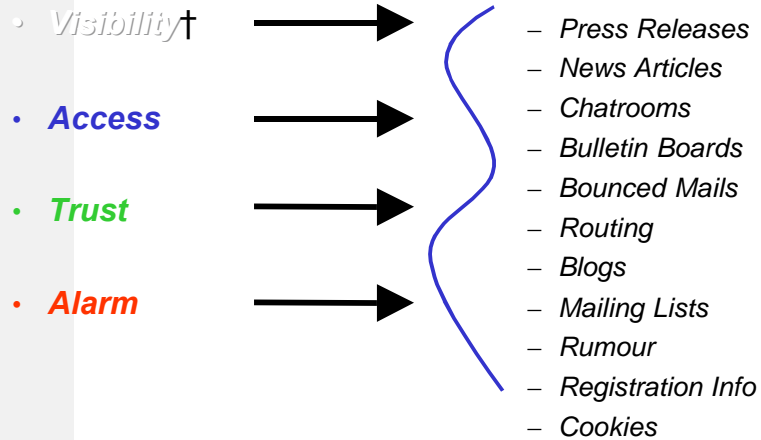
Copyright 2002 - Pete Herzog

## Wireless Security Presence



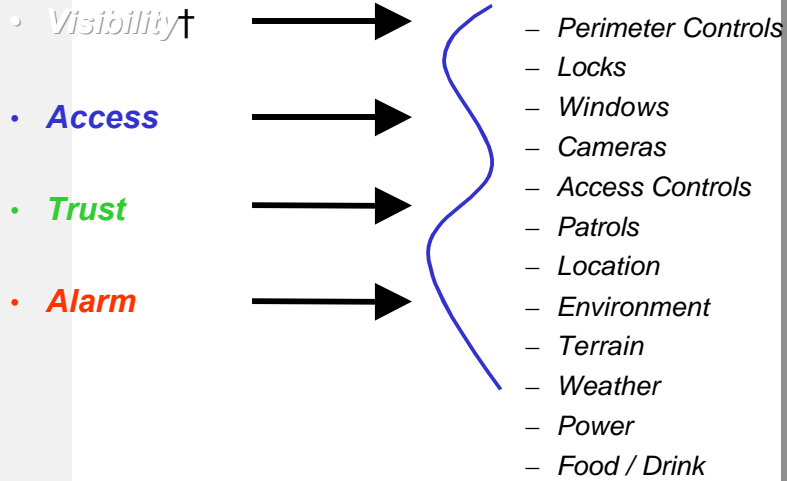
Copyright 2002 - Pete Herzog

## Information Security Presence



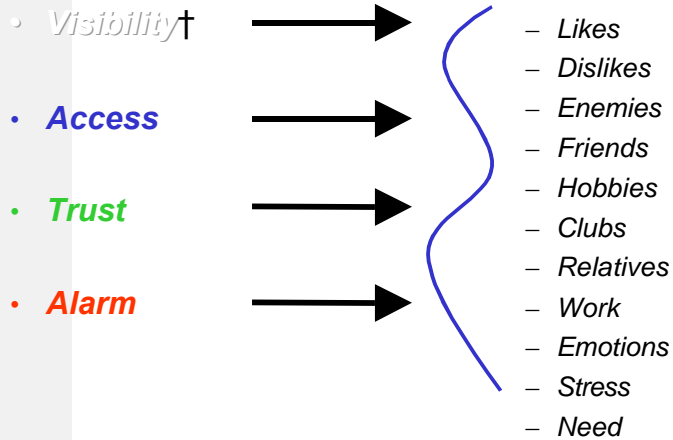
Copyright 2002 - Pete Herzog

## Physical Security Presence



Copyright 2002 - Pete Herzog

## Training Security Presence



Copyright 2002 - Pete Herzog

*Better be despised for too anxious apprehensions, than ruined by too confident security.*

• **Edmund Burke**

Copyright 2002 - Pete Herzog

*You are a licensed safety inspector for an independent occupational safety consortium. You have been brought to a large factory to review the safety of their machines due to a high number of accidents.*

- List 10 questions you would ask the foremen of this factory.
- List 10 concerns the employees may have with the current rise in accidents.
- List 10 concerns the employees may have with the implemented changes.
- List 10 changes which would make the factory a safer place to work.

Copyright 2002 - Pete Herzog

## Security Responsibility

- Employees
- Equipment
- Data / Information
- Communications
- Business Processes

Copyright 2002 - Pete Herzog

## Safety Responsibility

- Employees
- Customers
- Partners / Resellers
- Strangers

Copyright 2002 - Pete Herzog

## Privacy Responsibility

- Employees
- Customers
- Partners / Resellers
- Strangers
- Business Processes
- Data / Information

Copyright 2002 - Pete Herzog

## Recovery Responsibility

- Equipment
- Data / Information
- Business Processes

Copyright 2002 - Pete Herzog

The atom, being for all practical purposes the stable unit of the physical plane, is a constantly changing vortex of reactions.

– Unknown

Copyright 2002 - Pete Herzog

## **Practical Internet Security Defined**

- Usability
- Business Justification
- Policy
- Legalities
- Promotion

Copyright 2002 - Pete Herzog

## Common Limitations

- People
- Management
- Public Acceptance
- Cost
- Durability
- Trends

Copyright 2002 - Pete Herzog

## People

- Weakest security link
- Need continuous security training
- May not be trainable
- Benefits motivated
- Move towards self-efficiency / patterns
- Have engrained patterns of right and wrong
- Come and go
- Leave freely every night with information in their heads which can't be controlled.

Copyright 2002 - Pete Herzog

## Management

- Need continuous security training
- Profit motivated
- Move towards profitability
- Have engrained patterns of right and wrong
- Large influence over others if perceptions are negative
- Leave freely every night with information in their heads which can't be controlled.

Copyright 2002 - Pete Herzog

## Public

- Difficulty in use
- Poor understanding of need
- Poor understanding of law
- Benefits motivated
- Move towards ??? speed / interest / etc.
- Large influence over others if perceptions are negative

Copyright 2002 - Pete Herzog

## Cost

- High cost of entry
- High maintenance costs
- Needs new procedures which will cause project delays and personnel hesitations
- Benefits are not always clear

Copyright 2002 - Pete Herzog

## Durability

- May age quickly
- May not properly scale
- May not be re-utilized (single intended use)
- May not be acceptable for many users

Copyright 2002 - Pete Herzog

## Trends

- Will affect initial costs
- Will affect maintenance costs
- May change public acceptance
- May change management acceptance
- May destroy current arguments for use

Copyright 2002 - Pete Herzog

There is nothing in the world that some man cannot make a little worse and sell a little cheaper, and he who considers price only is that man's lawful prey.

- **John Ruskin (1819 - 1900)**

Copyright 2002 - Pete Herzog

## Like Chapter One

- Screened Network
- DMZ Concept
- Simple Intranet Concept
- Limiting Listening Services

Copyright 2002 - Pete Herzog

## Internet Gateway

- No unencrypted / unauthenticated remote access
- Restrictions focus on “allow” and log it
- Decentralize
- Limit Inter-system Trust and Quarantine
- Install only applications / daemons you need
- Layers
- Invisibility
- Regular Testing
- Simplicity
- Price

Copyright 2002 - Pete Herzog

## Employees

- Decentralize authority
- Personal Responsibility
- Respect their Privacy
- Statistical Audits
- Empowerment
- Rewards
- Punishments
- Legalities in Policies

Copyright 2002 - Pete Herzog

## Mobile Computing

- Required containment measures
- System hardening
- Encrypted drives
- BIOS passwords
- Application Firewall
- Training
- Helpdesk / Support

Copyright 2002 - Pete Herzog

## Applications

- Simplicity
- Afterthoughts are generally insecure
- Business justifications
- Testing
- Validate all inputs
- Limit trusts (to systems and users)
- Encrypt data — don't hide it
- Hash it
- Server side is always more secure

Copyright 2002 - Pete Herzog

## End of Story

**Now that we have all this useful information, it would be nice to do something with it. (Actually, it can be emotionally fulfilling just to get the information. This is usually only true, however, if you have the social life of a kumquat.)**

Unix Programmer's Manual

Copyright 2002 - Pete Herzog