

# The Ultimate Security Risk: PEOPLE

Presented by  
**Andrew Plato, CISSP, CISM**  
President / Principal Consultant  
Anitian Enterprise Security

## Who am I?

- 15 years experience as software engineer, technical writer, systems administrator, and network security consultant.
- Certified Information Systems Security Professional (CISSP).
- Certified Information Security Manager (CISM)
- Qualified Security Auditor for PCI-DSS
- Expert with IDS/IPS, Microsoft Windows® security, and policy development.
- Author of numerous white papers and technical manuals on intrusion detection and protection systems.
- Worked on the development the BlackICE engine for Network ICE (now part of ISS RealSecure.)

# ANITIAN

## ENTERPRISE SECURITY

### My Perspective

I am a...

Geek



*Live Long & Prosper*

Business Executive



*Greed is Good*

Salesperson



*Always Be Closing*

Which makes me a *Security Realist*: Security & IT governance must be practical and reliable to be effective.

**ANITIAN**  
ENTERPRISE SECURITY

IT Audit & Assessment ♦ Security Integration ♦ Managed Security

### The Anitian Advantage

- ◆ Our strength is our focus and our diversity.
- ◆ IT Audit & Assessment
  - Assessment & audits
  - Compliance (NCUA, FFIEC, FISMA, PCI, GLBA, etc.)
- ◆ Security Integration
  - Firewall, IPS, proxy, NAC, Identity Management, SIM/SEM, etc.
  - Integration & optimization
- ◆ Managed Security
  - Managed firewall, IPS & more
  - Security Analytical Services (managed SIM/SEM)

**ANITIAN**  
ENTERPRISE SECURITY

IT Audit & Assessment ♦ Security Integration ♦ Managed Security

## Overview

- ◆ How we perceive risk & threats.
- ◆ How people react to threats.
- ◆ Dealing with human factors in risks management.
- ◆ Keys for managing risk and the people who must manage risk.

# How We Perceive Risk & React to Threats

### **Securiness**

- ◆ Security has two elemental components:
  - A Feeling
  - A Reality
- ◆ Feeling secure can, at times, be equally as important as actually being secure.
- ◆ People evaluate security in two ways:
  - Instinctively
  - Logically

### **Security is All About Trade-Offs**

- ◆ Many factors compete for security: Money, convenience, time, acceptance, etc.
- ◆ Effectiveness is not a good measure of security.
- ◆ The best way to evaluate any new security safeguard is an analysis of the trade-offs:
  - Protection offered
  - Cost
  - Perception
  - Overhead to use & implement
  - Risks reduced or eliminated
- ◆ Risk is inherent in everything.

### The Five Realities of Security

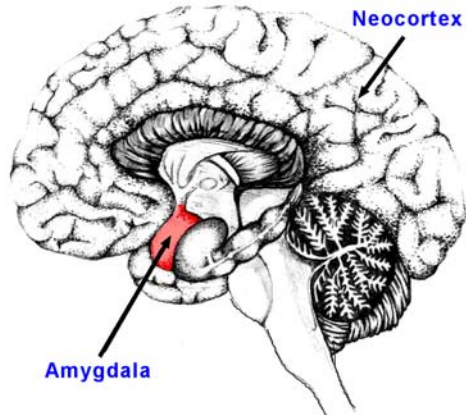
- ◆ Where we go wrong is when we start to ignore or delude ourselves about the realities of a threat.
- ◆ Five Security Realities:
  - Severity of the threat.
  - Probability of the threat.
  - Magnitude of the cost.
  - Effectiveness of countermeasures.
  - Ability to compare a threat to other threats.
- ◆ Risk = (Probability) \* (Impact)
- ◆ There is a finite number of risks, threats and vulnerabilities are practically limitless.
- ◆ People are a risk.

### Statistical Reality

- ◆ Chances of dying from:
  - Cancer 1 in 5
  - Heart disease 1 in 8
  - Drowning: 1 in 7,972
  - Fall in the bathroom: 1 in 10,455
  - Lightning strike: 1 in 55,928
  - Terrorism: 1 in 88,000
- ◆ Exotic threats are interesting and make good drama, but are not realistically cause for concern.
- ◆ Mundane, often well-understood, persistent, slow-acting threats are the most likely to lead to problems.

### I Think, Therefore I Am Pwn3d

- ◆ Your amygdala is a primitive part of your brain that you share with monkeys, mice, and other mammals.
- ◆ Your neocortex is the big, rational part.
- ◆ Your instinctual mind works hundreds of times quicker.



### Psychology of Security

- ◆ It is human nature to:

Exaggerate	Downplay
Spectacular	Boring
Rare	Common
Personal	Anonymous
External, beyond your control	Internally, taken willingly
Widely discussed	Uncommon
Intentional	Natural
Sudden	Slowly over time
Affecting yourself	Affecting Others
New and unfamiliar	Familiar
Uncertain	Well understood
Directed against their children	Directed at themselves
Immoral	Moral
Unlike now	Like now

### **Intelligence Failures**

- ◆ **Most, if not all, security failures have a genesis in human error.**
- ◆ **Laziness, bureaucracy, bad attitudes and ignorance can create a toxic, culture that ignores the realities of security focusing instead on the feeling of security.**
- ◆ **Cognitive dissonance causes people to convince themselves everything is okay.**
- ◆ **IT departments must address the human elements of people interacting with systems.**
- ◆ **Likewise, it must adopt processes and procedures that develop an internal culture that reinforces good security practices.**

# **Dealing with Human Factors In Risk Management**

### Cultivate Security Personalities

- ◆ Certain people have personalities that are well suited to security roles:

Desirable	Not Desirable
Analytical	Impulsive, Reactionary
Creative	Follower
Flexible, Accommodating	Rigid, hostile to change
Open-minded	Conforming
Dependable	Predicable
Collaborative	Loner
Innovative	Status-quo
Process as a guide	Process is law
Self-made	Paper-certified
Passionate	Obsessed with security
Diplomatic	Confrontational
Strategic, goal-oriented	Tactical, event-driven

### Lease Some Eyeballs

- ◆ Peer review is a fundamental component of all technical and scientific efforts.
- ◆ Its not just enough to have somebody look over your work, you need independent eyeballs.
- ◆ Managed security providers can offer a lot more than just saving money – they can mitigate human risk factors.
- ◆ Get your firewall and other key security components managed.
- ◆ Conduct regular assessments & audits of your infrastructure.
- ◆ Automate responses and alerting.

### Reason Reasonably

- ◆ **Be on the watch for behaviors that reinforce bad reasoning or faulty decision making:**
  - ◆ Optimism bias: *"We're okay because nothing bad has happened recently."*
  - ◆ Anchoring: *"We've always used XYZ and it works so we'll continue to use that."*
  - ◆ Bandwagon: *"Well, Big Boy Corporation uses this, so it must be good for us as well."*
  - ◆ Rigidity: *"We're a XYZ shop and we only use XYZ products and will not consider anything else."*
  - ◆ Inability to Assess Quality: *"They're all about the same so it doesn't matter what we use."*
  - ◆ Emotional Attachment: *"XYZ is better than ABC because I don't trust ABC to do what I want."*

### Simplify IT

- ◆ **Complex systems are:**
  - **More likely to fail.**
  - **More likely to get hacked**
  - **More likely to be poorly managed**
  - **More likely to cost you a fortune to maintain.**
- ◆ **Simplicity does not mean crude or rudimentary.**
- ◆ **Complexity can give people a false sense of importance.**
- ◆ **Simple solutions and architectures leave less room for human error.**

### **Blah Blah Blah Blah**

- ◆ Your greatest resource for understanding risks in your environment is the people that work there.
- ◆ If you get people talking, they will tell you almost anything – including exactly what risks are present.
- ◆ The Five Golden Questions:
  - What are you? What is it?
  - What are you doing? What does it do?
  - How do you work? How does it work?
  - What is your purpose? What is its purpose?
  - Why are you here? Why is it here?

### **To Err is Human**

- ◆ It does not matter how smart or dilligent you are, we are all dumb at some level.
- ◆ Automate security responses and management as much as possible.
- ◆ Deploy active defenses that can immediately respond to internal and external risks.
- ◆ Automate data collection, storage, analysis and disposal as much as possible.
- ◆ Automate Identity management where possible.
- ◆ Practice *least-privilege*. If a user does not require access to do their job, they should not have it.

### **Develop a Security Awareness Program**

- ◆ People evaluate security constantly, and will discount it if they don't see it as a priority.
- ◆ People will almost always take the path of least resistance to get their job done.
- ◆ A security awareness program must constantly sell, and resell good practices to everybody in the organization.
- ◆ Mistakes are opportunities to learn and grow...but repeated mistakes are evidence of an endemic fault that needs repair.
- ◆ Make security a *pervasive concern* for the business...but not an obsession.

### **Build a Strong Internal Culture**

- ◆ The internal culture of your organization can have a profound impact on you organization's ability to:
  - Adapt to changes
  - Recover from an attack or disaster
  - Implement security safeguards
  - Make decisions about security
- ◆ Culture is more than foosball and free pop:
  - Openness & honesty
  - Access to management
  - Expectation of excellence
  - Respect for strategic goals
  - Willingness to change

### **Be Curious, Kind, and Suspect**

- ◆ Security people need to think about those unlikely possibilities.
- ◆ A good security person has three core qualities:
  - Curious, about technology, process and people
  - Kind to people, the business and its needs.
  - Suspect of everything.
- ◆ But there is a fine line between risk analysis and obsession and creepiness.
- ◆ Доверяй, но проверяй.
- ◆ Don't Be: paranoid, obsessive, rigid – these are the qualities of an immature security person.

### **Be the Wind**

- ◆ People have a natural resistance to change, especially when it comes to security.
- ◆ It is much easier to complain about change than accept it and grow and learn.
- ◆ Growth means change.
- ◆ The stiff tree breaks in the wind.
- ◆ *Be the wind, not the tree. Persistent, adaptive, fluid.*
  
- ◆ *People are the #1 risk to your security – if you cannot change and adapt to handle human risk factors, you'll never be secure or compliant.*

**Thank You**

**You can get a copy of this presentation off  
the Anitian web site at:**

**[www.anitian.com/corp/papers](http://www.anitian.com/corp/papers)**

**My Contact information:**

**Andrew Plato, CISSP, CISM, QSA  
President / Principal Consultant  
Anitian Enterprise Security  
andrew.plato@anitian.com  
503.644.5656**