



System Integrity

Why Policies Will Fail ...
... unless you build
A Culture of Security

Anton Aylward, CISSP
System Integrity



Insider are the Real Threat

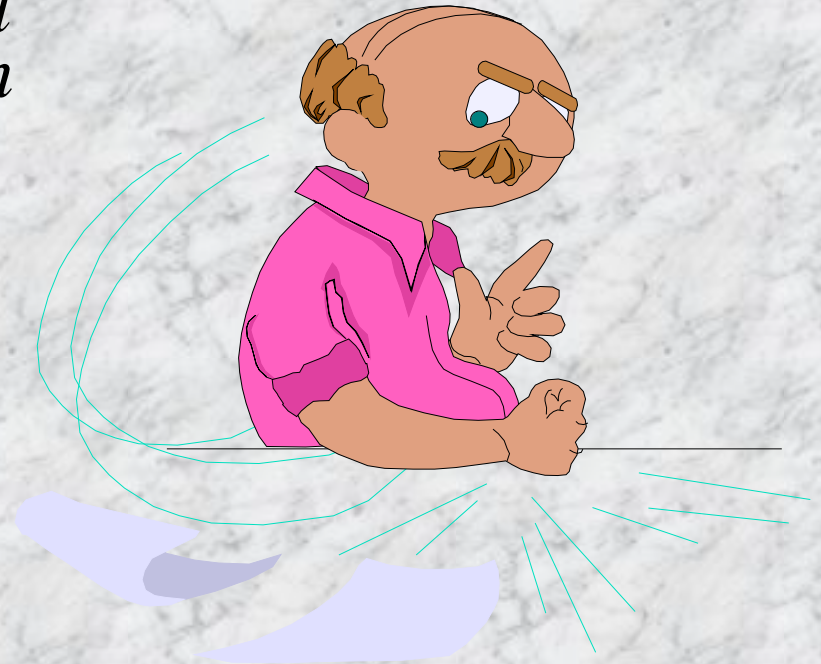
- Anecdotal Evidence
- Hard Evidence From The Outside World
- Hard Evidence From The IT World



Inside Threats: Anecdotes

“Are you telling me I can’t trust my own people?”

He was a good, practical manager who dealt with reality as he saw it and the bottom line, and didn't have time for this 'touchy-feelie' psychology nonsense, who managed by intimidation, yelling and guilt-tripping.





Inside Threats: Anecdotes

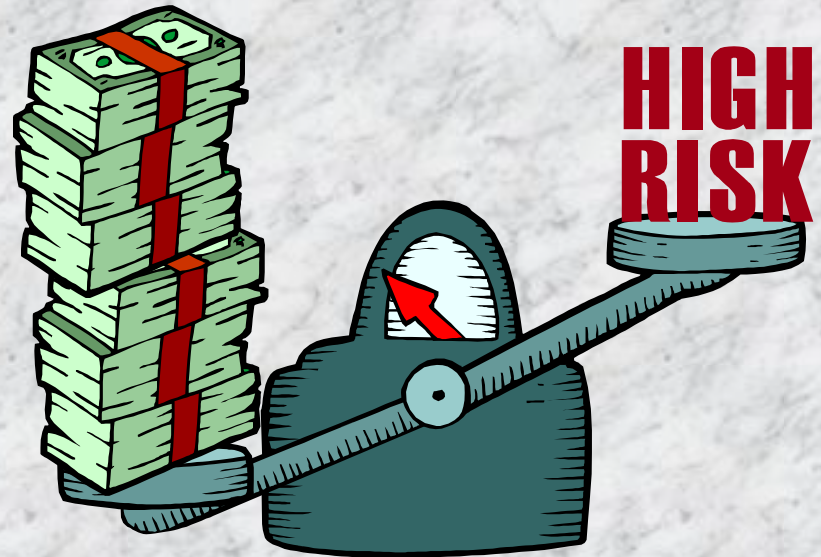
- Can you trust your own people ...
 - ⇒ Not to make typing mistakes?
 - ⇒ Not to make filing mistakes?
 - ⇒ Never to fall ill?
 - ⇒ Never to have family problems?
 - ⇒ Never to have financial problems?
- And Also ...
 - ⇒ To come to you with all their personal, financial and emotional problems?
 - ▶ Because they might impact the organization



Inside Threats: Anecdotes

“The basic motivation is fear”

The employees are guided in virtually every choice through anticipation of the negative consequences of their actions: “will my boss be mad?” “Will everyone think I’m incompetent” and most important, “Will it reduce my annual bonus?”





Inside Threats: Anecdotes

What do these have in common?

- Lack of Trust
 - The “bosses” don’t trust the “workers”
 - The “workers” don’t trust the “bosses”
- What kind of *Culture* is this?
 - Fear Uncertainty and Doubt



Hard Evidence From The Outside World

- People we thought we should be able to trust but couldn't

Richard Nixon

Aldrich Ames

The Walker family

Robert Hansen

Institutions we should be able to trust

Government Agencies

Religious Organizations

Its not the organization we don't trust, it's the people
in it

... therefore ...



Hard Evidence From The Outside World

- Its people that are the problem
 - ⇒ Not Policies
 - ⇒ Not Technology
- People need to be ...
 - ⇒ Understood as individuals and groups in their cultural settings
 - ⇒ Managed
 - ⇒ Monitored

“If you think technology can solve your
problems,
then you don't understand technology
and you don't understand your problems”
-- Marcus Ranum



Hard Evidence From The Outside World

- Robert Hansen, FBI
 - ⇒ Betrayed secrets over a 15 year period
 - ⇒ FBI paid \$7 million to get his KGB file
 - ⇒ KGB paid him over \$1.4 Million
 - ⇒ Lived a suspiciously extravagant lifestyle
 - ▶ ... but no-one suspected him
- Aldrich Ames, CIA
 - ⇒ Saw CIA wasn't faithful to double agents,
 - ▶ ... but KGB was
 - ⇒ KGB paid him over \$2 Million



Hard Evidence From The IT World

■ Distributed Denial of Service Attack Date: 8th Feb 2000

- ⇒ MafiaBoy took down Yahoo, E-bay for 4 hours
- ⇒ A system administration error took down E-bay for 8 hours

■ Full backup means full restore

- ⇒ IT manager demanded full backups
- ⇒ Business Process required extraction of single file
 - ▶ SysAdmin typo overwrote whole system

“Never attribute to malice what can be adequately explained by stupidity”



Hard Evidence From The IT World

■ Consider:

⇒ All successful outside attacks are the result of inside problems

- ▶ Lack of adequate protection
- ▶ Lack of correct configuration
- ▶ Lack of testing & checking
- ▶ Lack of awareness of issues - threat, vulnerabilities, techniques
- ▶ Lack of identification of assets
- ▶ Lack of appropriate business processes
- ▶ Lack of instruction & training

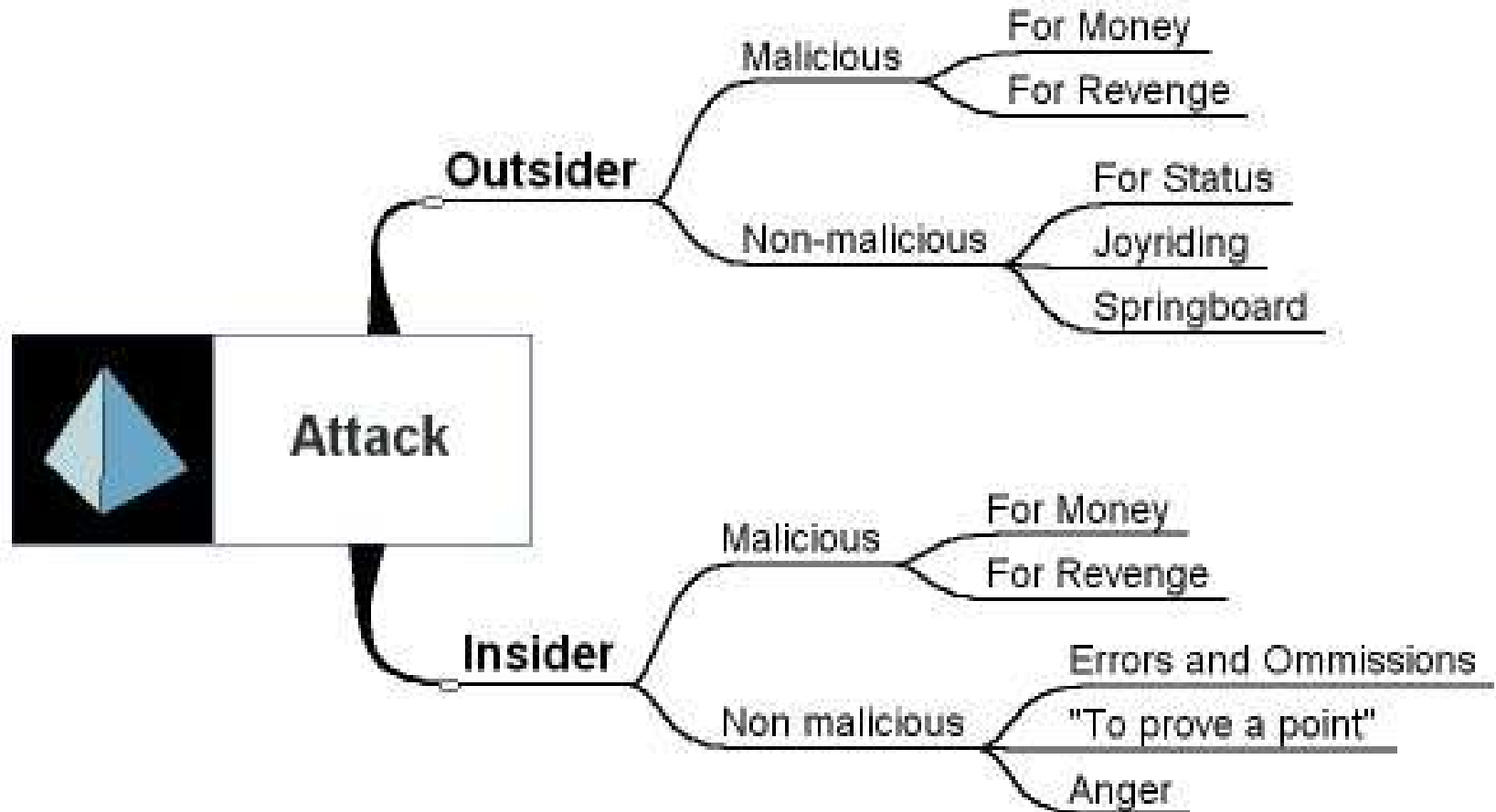
■ These are *People Problems*

- ▶ They happen because there isn't a "culture" that values security.

Talking about security doesn't mean you value it
Ineffective security proves you don't really value it



Insiders: Threat Modes





Insiders: Advantages

- Insiders have many advantages over outsiders
 - ⇒ They are already behind the firewall
 - ⇒ They know where everything is
 - ⇒ They can cover their tracks better
 - ⇒ They may have very personal motives
 - ⇒ They are already “trusted”



Insiders: Hidden Threats

- Management
 - ⇒ Lack of commitment
 - ⇒ Lack of demonstration of commitment
 - ⇒ Poor communication
 - ⇒ Ignorance of risks and issues
- Users
 - ⇒ Subverting security controls “to get the job done”
- The IT Department
 - ⇒ Obsession with technology
 - ⇒ Lack of understanding/ respect for
 - ▶ Business Issues
 - ▶ End Users



Insiders: The BIG problem

“Security? That’s not my
job”

OH YES IT IS !

- Board of Directors
- Executive management
- Line management
- Planners
- Auditors
- Financiers
- Project managers
- Supervisors
- Programmers
- Clerks
- Cleaners
- Janitors



Why Bother?

- People are a Company's Greatest
 - ⇒ Asset
 - ⇒ Liability
- Asset because ...
 - ⇒ You can't do without them!
- Liability because ...
 - ⇒ You can't do without them!
 - ⇒ If you don't trust them, you can't trust them
 - ▶ Trust is both ways



Why Bother?

■ ROI of Trust

- ⇒ No need to micro-manage
- ⇒ No need to overly specify
- ⇒ “Self monitoring”
- ⇒ Use their initiative
- ⇒ “Common Sense”
- ⇒ Less paranoia
- ⇒ “Happier Workplace”

 Improved Productivity



Why Bother?

■ Why is **TRUST** important?

In order to function, any community or organization must have sufficient trust to enable its members to share resources while preserving:

- Integrity
- Confidentiality
- Availability

Building A Culture Of Trust

... what's in it for me ?

... what's in it for my company ?

... what's in it for my country ?

... what's in it for humanity?



What do we mean by ...

- Culture
- Trust
- Security
- Ethics



What do we mean by “Culture”

- NOT: literature, opera, ballet
- “Normative Behaviour”
 - ⇒ Acceptable to and expected by the group
 - ⇒ Reinforced by the Group
 - ▶ Monkeys & The Fire Hose
 - ▶ Publishing Web logs
- Unstated Rules
 - ⇒ “Because God Says So”



What do we mean by “Culture”

Some cultures that place a great emphasis on Trust and Security:

- High Government
- The Military
- Police and Justice Systems
- Other Security Services
- Infrastructure Providers



What do we mean by “Culture”

“I firmly believe that any organization in order to survive and achieve success, must have a sound set of beliefs on which it premises all its policies and actions. Next, I believe that the most important single factor in corporate success is faithful adherence to those beliefs. Finally, I believe if an organization is to meet the challenge of a changing world, it must be prepared to change everything about itself except those beliefs as it moves through corporate life.”

-- Thomas Watson, Jr



What do we mean by “Trust”

- Dictionary:
 - ⇒ Confidence, reliance, dependability
- Based on ...
 - ⇒ Experience & Evidence of behaviour
 - ⇒ Word of others - references
 - ⇒ Personal relationships
- Easily Lost
- Emotional ??



What do we mean by “Ethics”

- Acceptable and Unacceptable Behaviour
- Right and Wrong beyond the law
 - ⇒ Values not Rules
- Hierarchy of Loyalties
 - ⇒ Company
 - ⇒ Country
 - ⇒ Humanity
- “Live with yourself”
- Very culturally dependant

“If people are only good because they fear punishment and hope for reward, then we are a sorry lot indeed.”
-- Albert Einstein



Ethics: Values or Rules?

- Need rules to provide a framework
 - ⇒ Constrain those who would take advantage
- But
 - ⇒ Rules have loop-holes
 - ⇒ They are obvious constraints
- Evidence in business world:
 - ⇒ People spend time trying to bypass rules

Ethics Toolkit for Managers:

<http://www.mapnp.org/library/ethics/ethxgde.htm>



What do we mean by “Security”

Its important to have a clear understanding of the objectives

We DON'T Mean

- Keep the hackers out
- Install firewalls and IDS and biometrics
- Run “risk assessments”

**“Don't Confuse Motion With Action”
- Hemmingway**



What do we mean by “Security”

We DO Mean

- Preserve the **INTEGRITY** of the resources & assets of the enterprise.
 - Keeping key resources & assets **CONFIDENTIAL**
 - Ensuring the resources & assets are **AVAILABLE** for the business functions of the enterprise
 - ... *and be able to show we have done this to the Auditors ..*
- “Peace, Order and Good Governance”**



Specifics

- **Baseline**
 - ⇒ Things to put in place to start with
- **High Risk Situations**
 - ⇒ Things that need heightened awareness
- **How to Manage for Security**
 - ⇒ Making it work day by day
- **How to Hire For Security**
 - ⇒ The right people



Specifics: Baseline

- You **must** have a baseline in place
 - ⇒ **Good Practice and Due Diligence**
 - ⇒ **Policy & Procedures**
 - ▶ ... define expectations
 - ▶ ... define escalation procedures
 - ▶ ... define remedial action (rewards/punishment)
 - ⇒ **Communication, Awareness & Training**
 - ▶ Is Ignorance an excuse? Yes.
 - ▶ Reinforcement
 - ⇒ **Attitude**
 - ▶ People matter
 - ▶ Quality matters



Why Policies & Procedures are Important

- Define what is:
 - ⇒ Expected behaviour
 - ⇒ Acceptable and unacceptable behaviour
- Consistency of Action
- Basis for ...
 - ⇒ Budget
 - ⇒ Disciplinary Action
 - ⇒ Avoiding liability/ negligence
 - ⇒ Economy of scale
 - ⇒ Measuring progress
- Demonstrate
 - ⇒ Compliance
 - ⇒ Quality

Don't wait until an incident occurs and try to figure out how to deal with it "on the fly"



Specifics: High Risk Situations

- Employee Termination
 - ⇒ Exit Interview
 - ⇒ Recover property - physical and intellectual
 - ⇒ Change Access Codes
- Mergers
- Disputes
- Creativity
 - ⇒ For some people, ideas matter most!



Specifics: How to Manage for Security

- Security is a **Management** issue
 - ⇒ Without commitment from the board and executive there is no belief that security matters
- **Security** is **NOT** an IT issue
- Training & Orientation
- Monitoring
- Enforcement

All this means **BUDGETING** for security



Specifics: How to Hire For Security

■ DO's

- ⇒ Check references
- ⇒ Check reputation
- ⇒ Have all the legal documents
 - NDA
 - Sign-off on understanding P&P

■ DON'T's

- ⇒ Hire hackers
 - “Ethical Hacker” = “Ethical Thief” or “Ethical Joyrider”



How to Fire for Security

- Have a formal termination procedure
 - ⇒ Exit Interview
 - ⇒ Recover property - Physical & Intellectual
 - ⇒ Change access codes, passwords
 - ▶ Building, parking, voice-mail, alarm
 - ⇒ Cancel outside accounts and memberships
 - ▶ Gartner, health-club, credit reports
 - ⇒ Sign Non Disclosure and other releases



Solutions:

POLICIES

Yes, you **MUST** have Policies!

Yes, you **MUST** communicate the policies & promote understanding of them

Yes, you **MUST** enforce the policies.

**“Don’t Confuse Motion With Action”
- Hemmingway**



Solutions:

POLICIES

Yes, you **MUST** have Policies!

Yes, you **MUST** communicate the policies & promote understanding of them

Yes, you **MUST** enforce the policies.

You **MUST** conduct security awareness training

BUT



Solutions:

Policies are Not Enough

You **MUST** have technical enforcement of policy

You **MUST** have “Defense in Depth”

You **MUST** have regular “audits”.

You **MUST** have regular awareness training

You **ABSOLTELYMUST** build ...

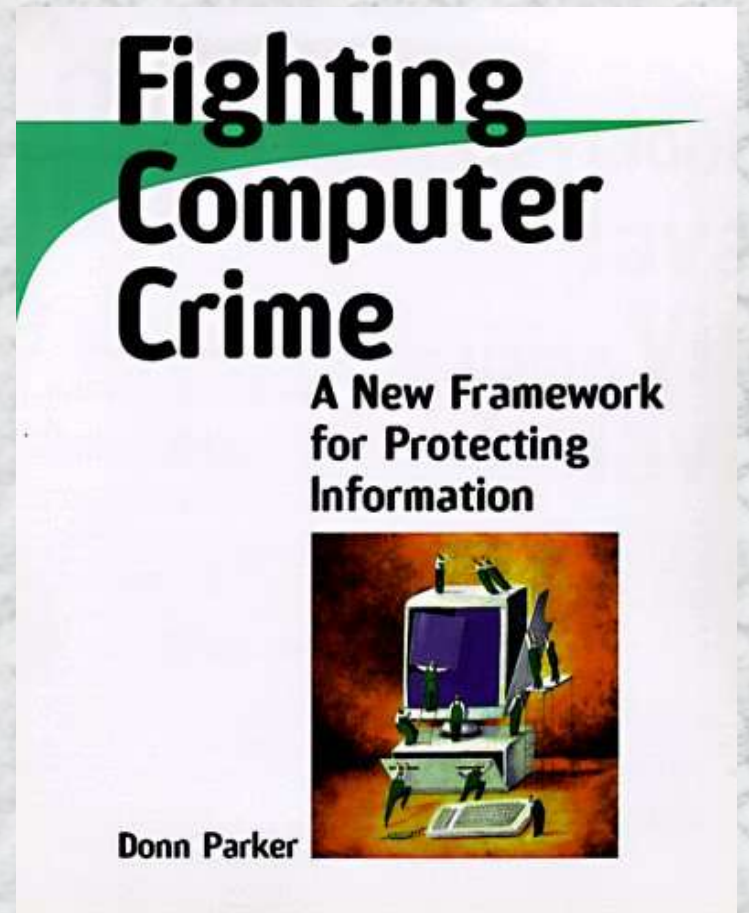
A Culture of Security



Recommended Reading

- “Fighting Computer Crime” - Donn Parker
- ISBN 0-471-16378-3

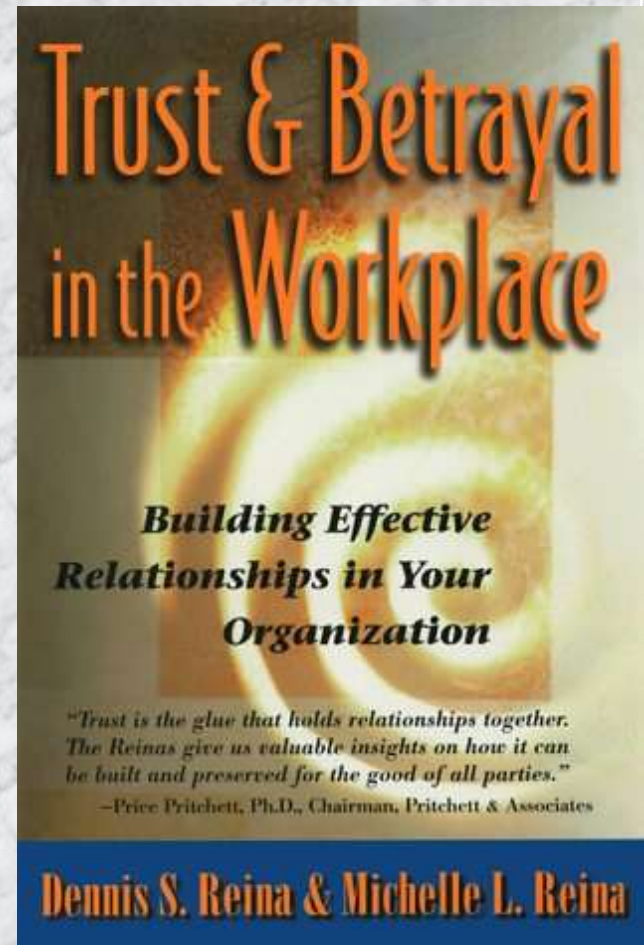
If I have to recommend just one book on Information Security it is this one.





Recommended Reading

- “Trust & betrayal in the Workplace”
- ISBN 1-576-750-70-1
- Managing expectations & boundaries
- Practical exercises





Recommended Reading

- **The Organizational Culture Perspective**
- **ISBN 0-534-10918-7**

Out of Print



Contact Information



System Integrity

“Security is not something that comes in a self-contained box. It requires a conscientious and continuous commitment that permeates every aspect of your enterprise and strategies. It is about understanding risks and managing them”

Anton J Aylward, CISSP CISA

aja@si.on.ca

<http://www.si.on.ca>

(416) 497-0201