



System Integrity

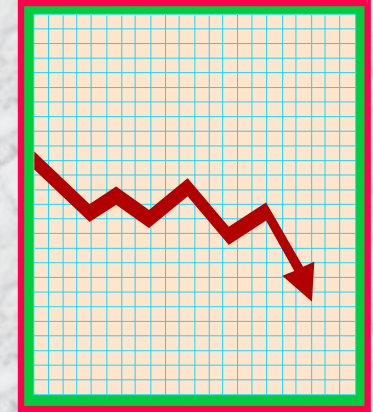
Penetration Testing Is A Bad Idea

Anton Aylward, CISSP, CISA
System Integrity



What are you trying to test?

- Can hackers break in?
 - You can't prove a -ve
- Your firewall works?
 - But is it configured?
- Your IDS works?
- Your response system?
- You've shown "due diligence"?





Penetration Testing

① **There's no such thing as "Ethical Hacking"**

Would you employ an 'ethical arsonist' to test your home smoke detector?

- ⇒ Ethical burglar to test your home security
- ⇒ Ethical murderer as a bodyguard
- ⇒ Ethical terrorist as an airport guard



Penetration Testing

② **It doesn't simulate a 'hacker'**

- It doesn't simulate their motives
- It doesn't simulate their timescales
- It may not simulate their methods

A hacker can spend weeks at \$0/hr in the intellectual challenge of writing an exploit, positioning it and deploying it. For this, he gets viewed as a “security guru”!

- Knowing how to break-in doesn't mean you know how to defend.



Attack Taxonomy

- Internal
 - ⇒ structured or unstructured
- External
 - ⇒ structured or unstructured
- Network based
- Application based
- Social based
- Natural/Man-made disasters
 - ⇒ fire, flood, wind, power, impact, theft



Penetration Testing

③ **It addresses less than 5% of security risks**

- It only looks at external interfaces
- Most security problems are internal
 - Errors and omissions
 - Lack of policy & procedure
 - Disaster Recovery and Business Continuity
 - Insider Threats
 - **Fragile Architecture**



Penetration Testing

④ **It should be the last thing you do**

- ... **After** making the changes recommended by an audit of the perimeter configuration
- ... **After** making the changes recommended by an audit of the *internal* configuration
 - Because you need ‘defense in depth’
 - Because you **DON’T** want to find any vulnerabilities
 - Because its less risky this way
 - **Because its less expensive this way**



Penetration Testing

⑤ **It's not cost effective**

- A conventional audit will tell you more for less
 - Use a well established methodology...
 - CobIT
 - SSE-CMM
 - ... that matches your business processes
 - And audit will tell you about
 - Your internal risks...
 - Your IT processes
 - Good Governance & Practices
- **Better ROI**



Penetration Testing

⑥ **It focuses on the Technical, not the Business**

- The ‘drama’ appeals to the media
- Techies like to show off
- Most of your security problems aren’t technical
 - People
 - Legal and IP
 - DRP/BCP
 - Rights Management
 - Spam
 - Viruses & Worrms
 - E-Mail problems
 - OS Problems
 - Patches & Updates



Penetration Testing

Technical or Business?

- Losses at Enron, WorldCom, Parmalat, Nortel, Royal Dutch Shell, Royal Plastics etc had nothing to do with hackers breaking in
- Disclosures at XXX YYY ZZZ had nothing to do with hackers breaking in
- Most of your security problems aren't technical



Penetration Testing

- ⑦ **It only addresses the known, not the unknown or future exploits**
 - Its impossible to predict future InfoSec incidents based on past events
 - Pen-testing doesn't test your processes, only your defenses
 - ... and only your external, static, boundary defenses



Other Shortcomings

- Doesn't test forensics needed for possible follow-up (e.g. prosecution of hackers)
- Doesn't validate that the successful defenses follow the business requirements
- Doesn't test your hiring, training, dismissal and other "human factors" procedures
- Its not a continuous/feedback process



Why is Pen-Testing Popular?

- The Media
 - ⇒ Hackers make Headlines
- Its Dramatic
- Its Fascinating
- Its Fun! - *techies like it*
- It “Opens Doors” - *salesmen like it*
- Its easy to sell to people who don't understand the real issues
 - ⇒ Fear ... Uncertainty ... Doubt



The Big Downside

Penetration testing is “**avoidance behavior**”.

By focusing attention on outside threats the real and more complex problems, the internal problems of **IT governance**, business **needs** and **processes**, internal controls and oversight, **problem, change and configuration management** are all avoided.



What Should You Do?

- Perform a *simplified* Risk Assessment

WHY?

- Dealing with higher risk issues has better ROI
- Identifies **YOUR** real vulnerabilities
- Puts **YOU** in control of what gets fixed first

Avoid “One Size Fits All”



What Should You Do First?

■ Identify your assets

⇒ Computing assets

- ▶ including the ones you didn't know you had

⇒ Communication assets

- ▶ including the ones you didn't know you had

⇒ Data Assets

■ Assign Values

⇒ Monetary

⇒ Business Process Criticality



What Should You Do Next?

- Identify your business processes
 - ⇒ rate them by criticality
 - various metrics
- Cross correlate assets & processes
 - ⇒ matrix
- Identify what can go wrong
 - ⇒ What is the impact?
 - ⇒ What is the likelihood?
 - ⇒ How can it be mitigated?
- Define a “baseline”
 - ⇒ So you can show & measure improvements



Now you have the information

- **Plan**

- ⇒ What controls to put in place?

- **Do**

- ⇒ Put them in place

- **Check**

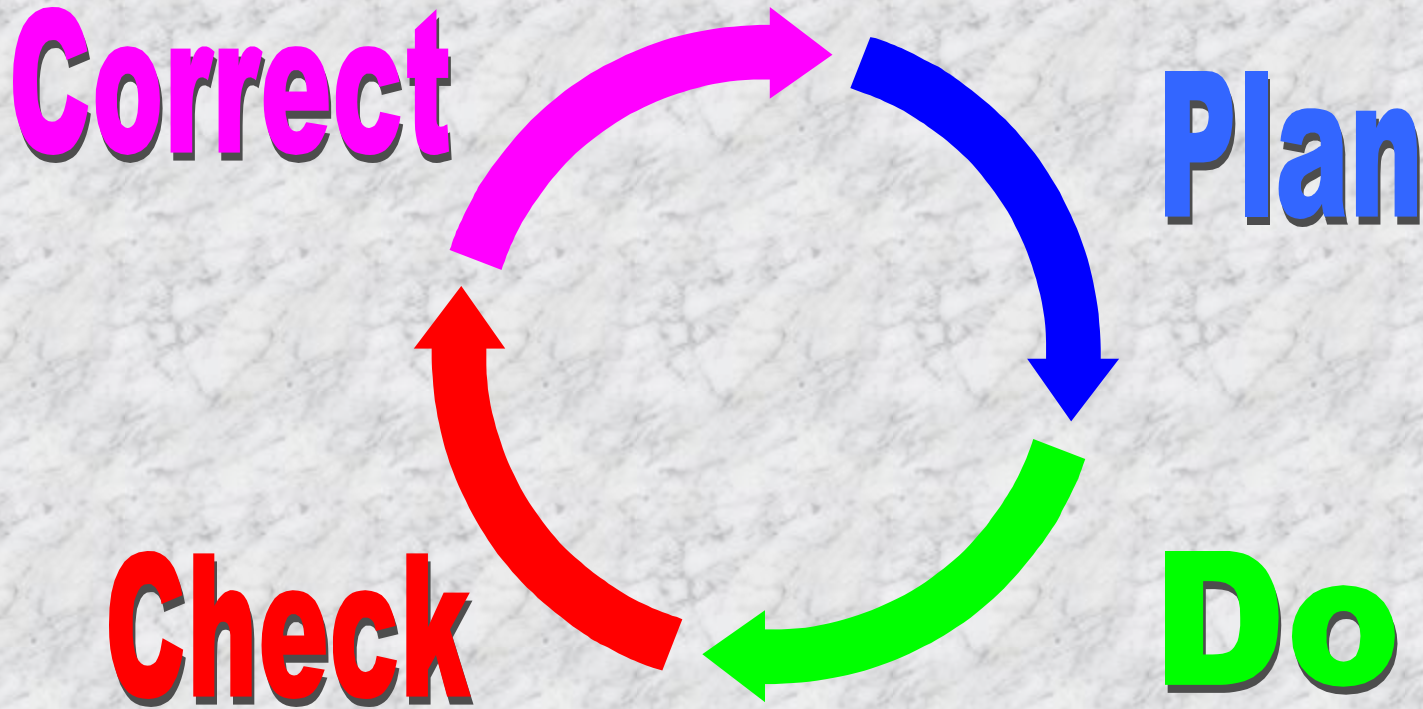
- ⇒ Do they work? What is missing?

- **Correct**

- ⇒ Keep doing it




Now you have the information



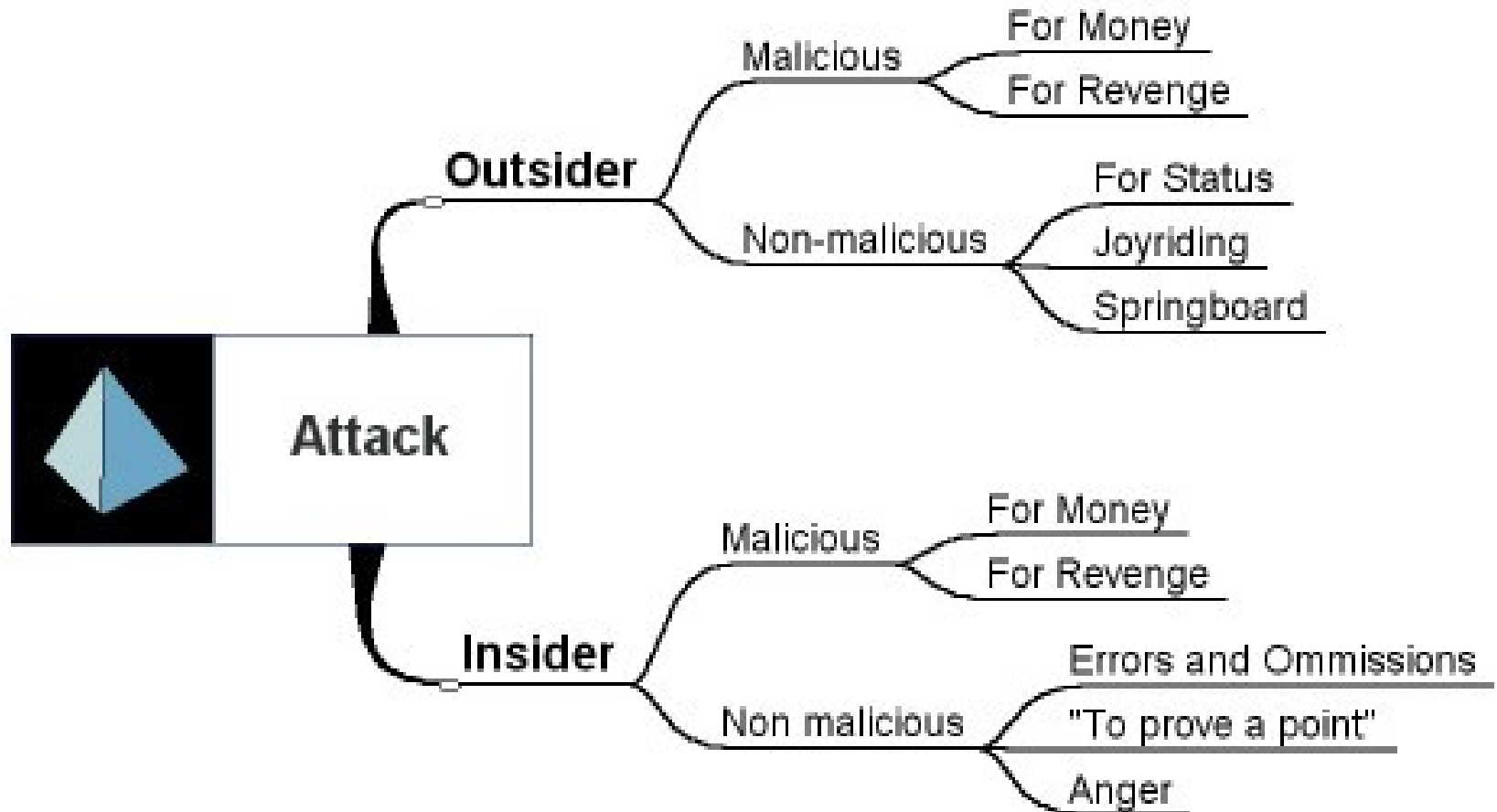


Things to Consider

- You only have control over your “inside”
- Most security problems are on the “inside”
 - ⇒ Configuration
 - ⇒ Change management
 - ⇒ Awareness
 - ▶ ... of the issues
 - ▶ ... of events
 - ▶ ... of what action to take



Inside or Outside Attacks





Inside Risks & Threats

- “Finger Trouble”
 - ⇒ Typos
 - ⇒ Too hurried to check
 - ⇒ Other Distractions
- Ignorance
 - ⇒ Miscommunication
- Frustration
- Malice
- Espionage
 - ⇒ Ames, Walker, Hansen





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”

Penetration Testing Doesn't Test Your Highest Risks



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



How to Approach Security Assurance

- ① Understand what you mean by “Security”
- ② Focus on Business not on Technology
- ③ Think in terms of Processes & Controls
- ④ Decide what Risks you can live with



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”



The Business of Security

- **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

These are all management issues



Management: 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"



Why Policies & Procedures are Important

Policies and Procedures are the basis for all processes and controls that determine that short and medium term operation of the organization



Management: High Risk Situations

- Employee Termination

- ⇒ Exit Interview

- ⇒ Recover property - physical and intellectual

- ⇒ Change Access Codes

- Mergers

- Disputes

- Creativity

- ⇒ For some people, ideas matter most!



Management: 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



Management: 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”



Management: 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

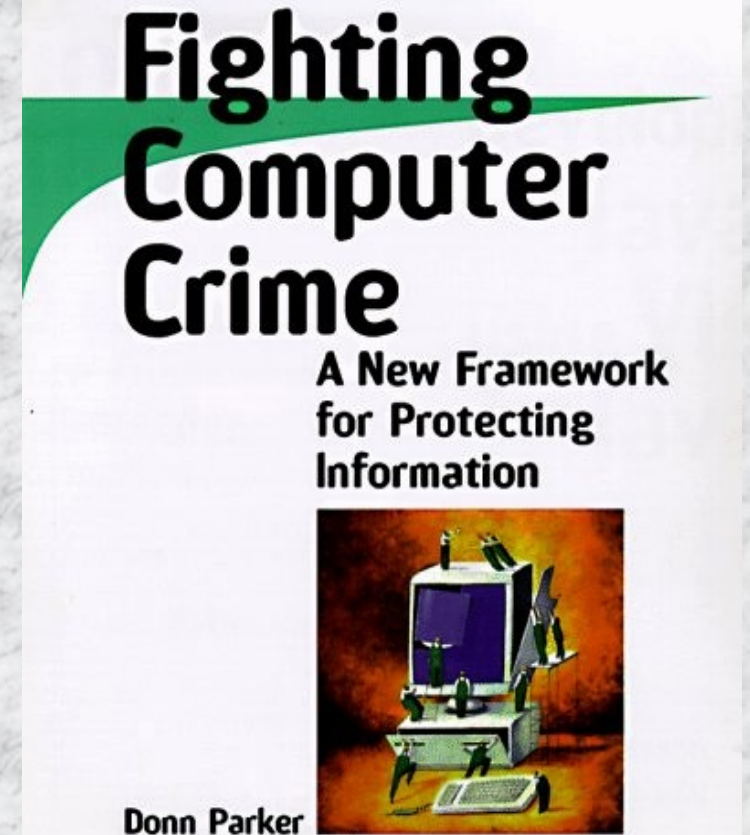
BUT



Recommended Reading

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

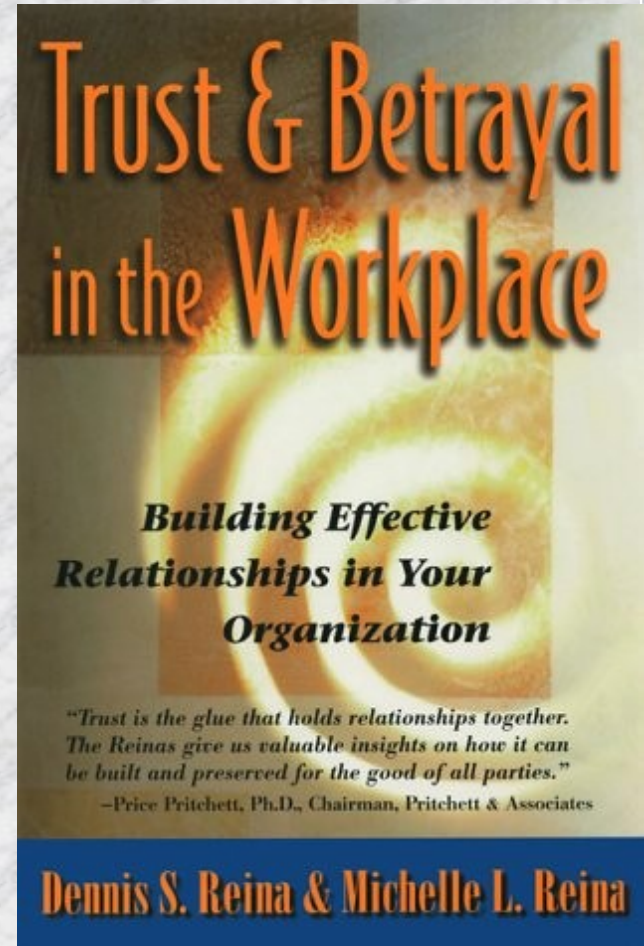
If I have to recommend just one book on Information Security it is this one.





Recommended Reading

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





Who do you Trust?

Web sites





Who do you Trust? Professional Certification



- Recognition
- Professional Ethics
- Accountability
- Methodology





Who do you Trust?

Professional Certification

- Recognition
 - By Community of Peers
 - By Means of Process
- Professional Ethics
- Accountability
- Methodology
 - Professional Process
 - Communication



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