



# **“Appropriate and Proportional Controls”**

**A Security Practitioner's Perspective**

# Introduction

- Who are we?
- Why are we here?
- Why do you care?

## Hints:

Alternate perspectives are a good thing.

Complementing resources to the organization.



# Agenda

- Security Risk defined (from our perspective)
- Three Myths of Control
- Appropriate and Proportionate (what does this mean?)
- Examples of Practical Security
  - Patch Management
  - Threat Management
- Closing Statements
- Q&A

# We Got Some Argot!

- **Control** - *The policies, procedures, practices and organizational structures designed to provide reasonable assurance that business objectives will be achieved and that undesired events will be prevented or detected and corrected. (COBIT)*
- **Appropriate** - *"Suitable for a particular person or place or condition." (dictionary.com) Management must understand the status of its own IT systems and decide what security and control they should provide. (COBIT Audit Guidelines)*
- **Proportionate** - *"Corresponding: agreeing in amount, magnitude, or degree" (dictionary.com) Ultimately, management must decide on the level of risk it is willing to accept. (Cobit Audit Guidelines)*
- **Reasonable Assurance** - *"A level of comfort short of a guarantee but considered adequate given the costs of the control and the likely benefits achieved" (auditnet.org)*
- **Risk** - *Nearly every page of the COBIT framework uses the word "risk" – but no definition is given. "The possibility of suffering harm or loss" (dictionary.com)*



Now for the Security Perspective...

# Security Risk

## Quantitative Analysis

Lots of equations and numbers...

- Dearth of applicable statistics
- Unquantifiable intangibles

Antivirus and electronic badges (lends itself to ROI)

## Qualitative Analysis

- Intentionally "imprecise"
- Useful for prioritization

Example: Information Leakage

# Qualitative Expanded

**Risk** = probability x impact

**Risk** = (threat x vulnerability x opportunity) x impact



In the *Risk* equation, the vulnerabilities and opportunities are most often unknown, and even impact is mostly a guess.

# An Example

Suppose a \$100 bill is left on a desk

- The vulnerability is a susceptibility to theft.
- The opportunity is relative to the lack of access controls around the desk and only useful for *known vectors* of access.
- The threat is a thief approaching the desk.



(Vulnerability and opportunity are not the same – consider an egg.)

# Imagine...

An unpatched stand alone PC containing nuclear arms confidential information in a locked room with 24x7 armed guard and biometric locks -- and only one person is allowed.

**Risk** = threat x vulnerability x opportunity x impact

**Risk** = 3 x 3 x 0 x 3

# Imagine...

That same PC is now connected to a public network.

**Now the opportunity is high also!**

**Risk = threat x vulnerability x opportunity x impact**

**Risk = 3 x 3 x 3 x 3**

# Security Risk - Essential for Advice

- Without a statement of risk, one cannot answer the question –  
“Is this control appropriate or proportional?”
- Formal, informal, detailed or “back of a napkin” – the risk must be defined.



# Three Myths of Control

The Myth of Prevention

The Myth of Perfection

The Myth of Provability

# The Myth of Prevention

“Bad things must be prevented”

**Not always.** If detection and correction is possible, prevention may not be the best approach. Examples:

Credit Card Fraud

Home Burglaries

Mild Illness

“Bad things can be prevented”

This is nearly always false. Examples:

Credit Card Fraud

Home Burglaries

Mild Illness

# The Myth of Perfection

“If a control isn't perfect, it is broken”

**This is nonsense.** Most of the controls we consider to be effective are not perfect, and it doesn't bother us.

Examples:

- Hand Sanitizer (Only kills 99.99% of germs on contact)
- Credit Card Authorizations (Billions in fraud annually)
- Front Door Locks (Numerous ways to break or bypass)
- Police Radar traps (less than 100%, but do reduce fatalities)

# The Myth of Provability

“How do you know...”

- Philosophical concepts aside, it is **impossible to provide absolute proof**, especially in a technology environment.
- Ken Thompson's 1984 article on subverting the C compiler  
<http://www.acm.org/classics/sep95/>
- 2005 Underhanded Code Contest  
<http://bingweb.binghamton.edu/~scraver/underhanded/>
- Firewall Configuration/Administrators

# Appropriate

- Will it have the desired effect?
  - Confiscation of nail clippers in airports
- Will it have undesirable side effects?
  - Screen Saver timeouts
- Is it feasible to implement
  - For example, PKI



# Proportional

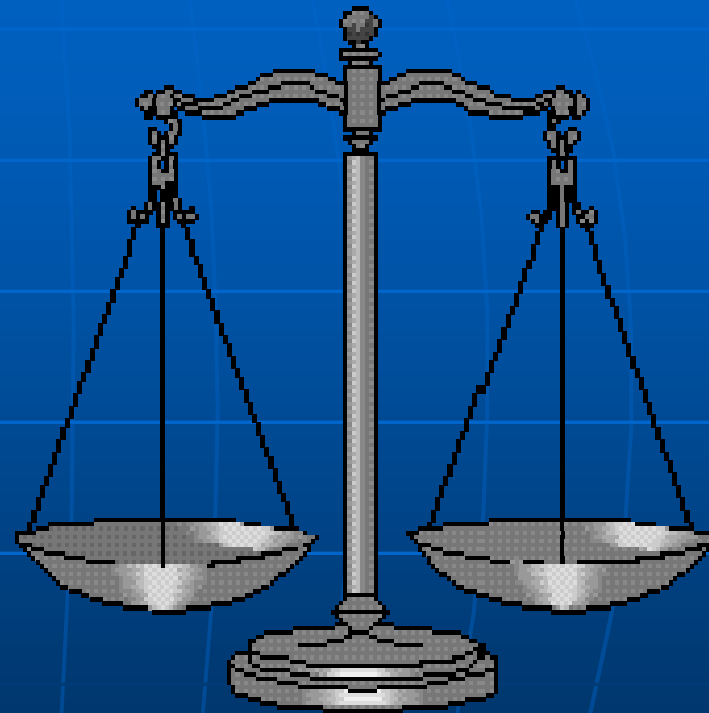
Relative to the risk:

- Is the cost reasonable?
  - \$100 lock on a \$5 bike
- Is the inconvenience reasonable?
  - Locking windows on a hot summer night
- Are the opportunity costs reasonable?
  - No signature needed for gas purchase



# Prevent or Detect?

- Do we have recourse?
  - Credit Card Fraud
- Can we survive an incident?
  - Public Relations
- Which is more practical?

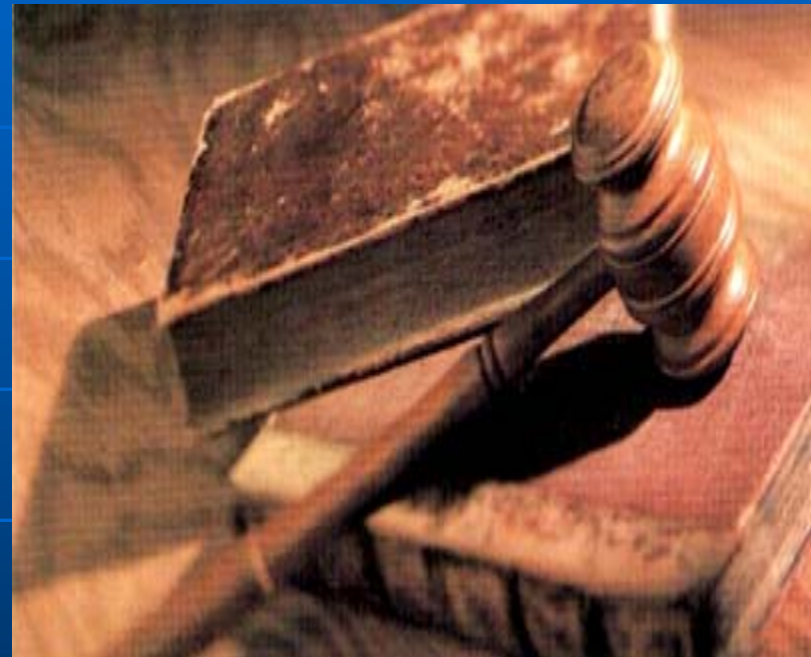


# Who Decides?

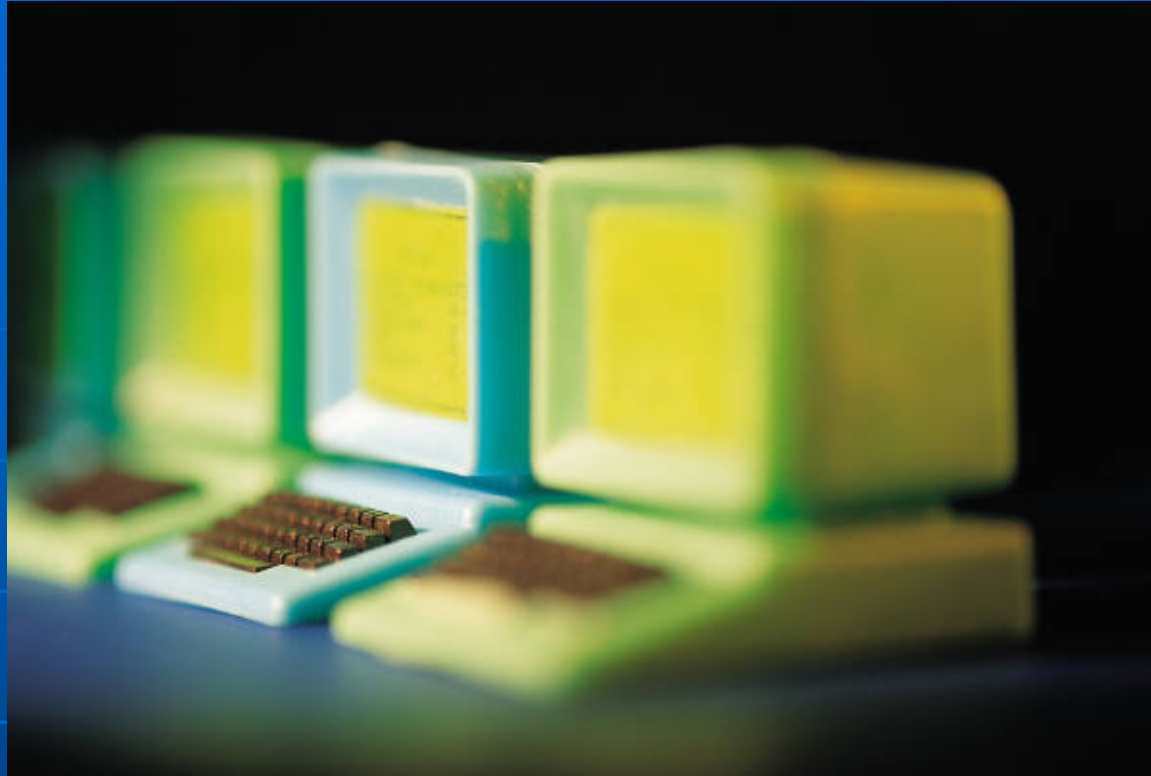
- Audit? – No.
- Security? – No.

**“Ultimately, management must decide on the level of risk it is willing to accept.”**

- Cobit Audit Guidelines



# Practical Examples



# Patch Management

Number One Appropriate Control for IT  
(from our perspective)

# Why Patch?



**Unpatched systems are the leading cause of system exploitation!**

# Patching: Number One Priority

- **Best bang for the buck, period...**
  - Minimizes opportunity
  - Minimizes potential likelihood of exploit
  - Minimizes potential impact
- **More important than...**
  - Business project deadlines
  - IDS/IPS (and most other security gizmos)
- **True defense-in-depth**
- **Establishes awareness and ownership**



# Is the Patch Program Appropriate to the Risk?

- **Business**
  - Can the business handle an outage (patch compatibility or malware related – which is worse)?
  - What is the exposure of the system in question?
- **Security**
  - What is the likelihood of the threat?
  - What is the potential impact?
  - How long of a “patch gap” can be tolerated?
- ***Bottom Line – doesn't require a fancy tool, just get it done!***

# Threat Management

# Protecting Against the Unknown

One of two options (or a mix of both)...

## Option 1:

Commercial “blackbox” solution – Intrusion Detection (IDS), Intrusion Prevention (IPS), filters, proxies, All-in-one, etc.

## Option 2:

Human Review – Aware People System (APS)

*Hint: Don't rely on technology alone...*

# Characteristics of IDS vs. APS

## IDS (etc)

- Packet contents
- Word or sentence
- Suitcases through X-ray
- Compares against signatures
- Some heuristics
- Plagued with false positives
- Never done tweaking
- Highly predictable

## APS

- Basic Communications
- Who is talking with whom?
- Suspicious characteristics (one-way tickets, no luggage, heavy coats in summer, etc..)
- Focus on behavior, not just data stream elements
- Trigger on the anomalous or unexpected
- Adaptive and unpredictable

# Example 1

- **MS Blaster Worm**
  - Symptom is "random pinging of Internet hosts"
    - **IDS** -> ICMP echo/reply is "normal" traffic
      - Possibly only key on the "volume" of traffic
    - **APS** would immediately wonder "why is this internal host pinging these external hosts?"
      - (Assumes some basic egress filtering)
        - Firewalls log outbound traffic, denying and logging any non-business attempts
      - Simple script on the logging host to alert us for X number of denied ICMP packets within Y minutes
      - We can always aggregate the data to catch the low/slow

# Example 2

## Mail Virus

- Symptom is "SMTP (tcp port 25) to internet hosts"
  - IDS -> SMTP thinks this is "normal" traffic
  - APS says, "Whoa! Why is this internal host attempting to use an external mail host? All of our boxes use our internal mailhost" **Hmmm....**
  - Assumes some basic egress filtering
    - Firewalls log outbound traffic, denying and logging any non-business attempts
    - Simple script on the logging host to show denied tcp port 25 connections

*Aware people with the right tools works best...*

# Computerworld says...

“Like other types of management software, SIM is only a tool. It can assist your security personnel in better securing the enterprise, but it’s not a replacement for their perception and skills.”

~ Computerworld

# Bruce Schneier says...

“You automate data collection, data correlation, data search – the tasks that are boring and suitable for computers. But you can’t automate intelligence, and you can’t automate creative thinking.”

~ Bruce Schneier – author and CTO at Counterpane Internet Security Inc.

# Do's and Don'ts

- Be practical and open minded – many times the informal solution is more “appropriate” and “proportional” than a formally structured commercial solution
- Don't dive deeper than necessary
- Avoid the Myths of Control
- Technology isn't always the answer
- Be positive, remember “no findings” is a finding

Q & A

It's a chicken!  
Open the gates and  
park it next to the  
big wooden horse!



Stacy.Bresler@pacificorp.com  
503.813.6430

Daniel.Marvin@pacificorp.com  
503.813.5375

Steven.Parker@pacificorp.com  
503.813.7224

Patrick.Miller@pacificorp.com  
503.813.7014