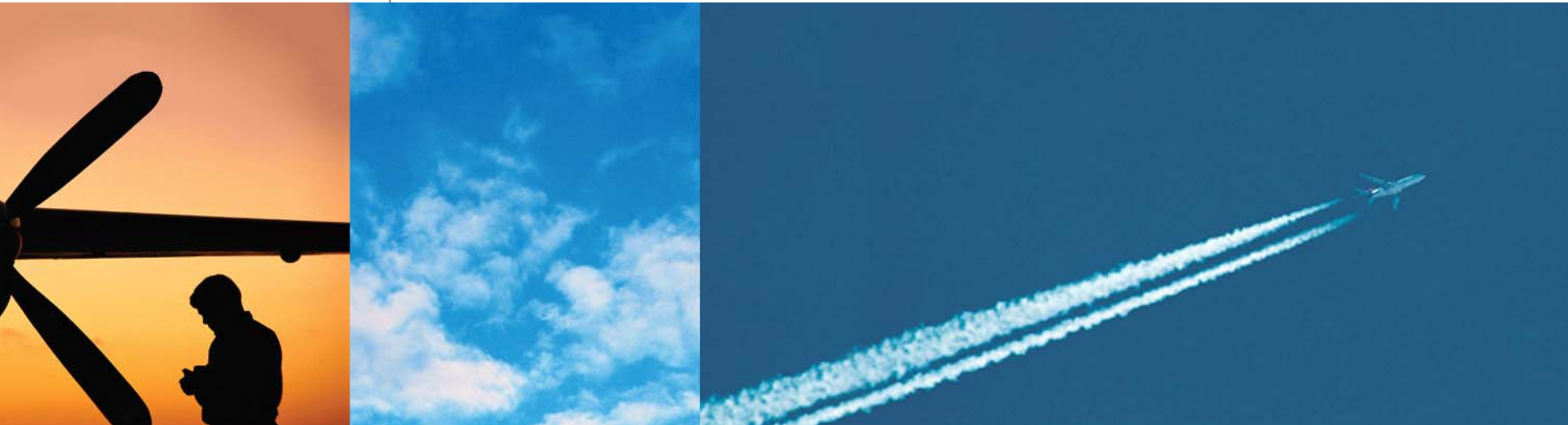




# *Secrets of Superspies*

**Ira Winkler, CISSP, CISM**  
**[iwinkler@csc.com](mailto:iwinkler@csc.com)**  
**+1-410-544-3435**



EXPERIENCE. RESULTS.

# The Second Worst Spy in the World



# The Worst Spy in the World



# They are Everything You Want

- They kill people
- They blow things up
- They infiltrate enemy positions
- Their enemies fear them

## But...

- They kill people
- They blow things up
- Their enemies know who they are
- They always get caught

# How Can You Miss This?



# What Do Spies Really Do?

- They determine requirements
- They collect information
- They analyze information
- They re-evaluate their needs
- Collection is the apparent focus, but it is the requirements that are most critical

# Science vs Art

- Hackers like to portray themselves as “artists”
- Spies are “scientists”
- There is a repeatable process to what they do which is required for expertise
- Ability vs. Practice vs. Training
- You need two
- No training makes you dangerous

# Spies Protect Themselves From Other Spies

- Counterintelligence
- They know the tricks of the trade, so they know what to expect
- They know they have to be right 100% of the time, while their adversary just has to be right once
- There is nothing there about protecting computers for the sake of protecting computers

# The Key

- Spies focus on Information
- Technology is only important in that it provides access
- Different classifications get different levels of protection
- While there is tremendous threat, the actual losses are relatively small

# Risk

- Spies hate Risk

$$\text{Risk} = \left( \frac{\text{Threat} * \text{Vulnerability}}{\text{Countermeasures}} \right) * \text{Value}$$

# Risk Broken Down

- Threat – Who or What is out to get you
- Vulnerability – Your weaknesses that allow the Threat to exploit you
- Value – Value of your information or services at risk
- Countermeasures – Measures taken to mitigate the Risk

# What's Important to You?

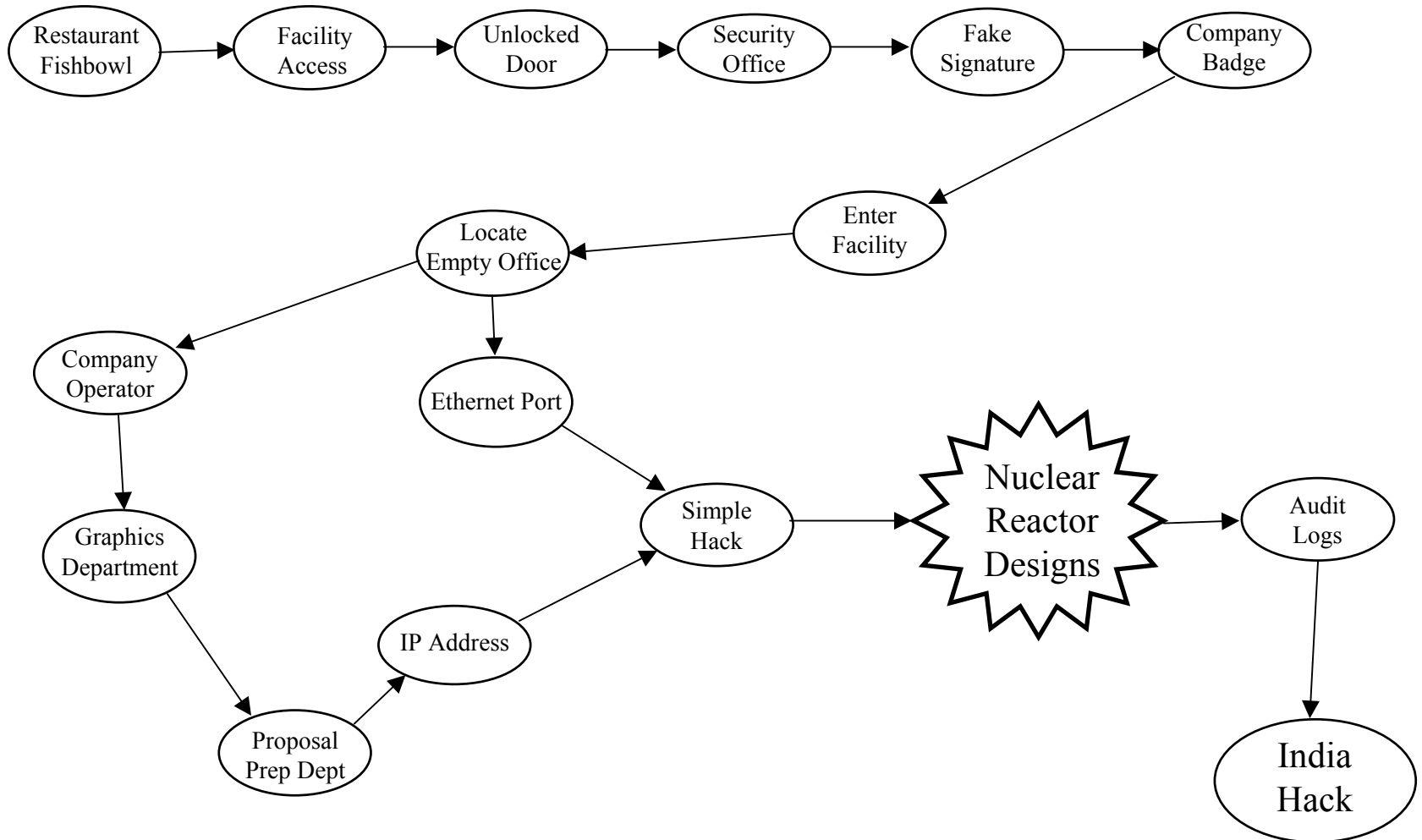
- People focus on the Threat
- Spies acknowledge the Threat is a given
- Threat is irrelevant
  - For the most part
- They focus on mitigating Vulnerabilities

# Case Study #1

- Compromise of nuclear secrets
- Full scale espionage simulation
- No holds barred attack
- Multi-faceted attack
  - Open source research
  - Misrepresentation
  - Walk through facilities
  - Internal hacking

# Background

- Organization is very large with a large central organization
- Had traditional security issues, but no major issues that they knew about
- Organization as a whole experienced massive layoffs
- Only one security manager at HQ, with an intern, and no unit security managers



# Results

- Nuclear reactor designs compromised
- Emerging technologies compromised
- Production potentially compromised
- National security implications
- It was extremely simple
- ID card was unnecessary

# Believe it or Not

- *Critical compromises accomplished within a half day*
- *No reports of any activities*
- *India hack was previously unknown*

## Case Study #2

- Placement of a person as a temporary employee in a high tech firm
- Full scale industrial espionage simulation
- No holds barred attack
- Multi-faceted attack
  - Open source research
  - Misrepresentation
  - Walk through facilities
  - Internal hacking
  - Internal coordination of external accomplices

# Background

- Company has many emerging developments
- Developments valued in excess of \$10 Billion by Wall Street analysts
- Company has experienced several cases of industrial espionage
- Research mentality of openness causes an operational security nightmare
- Security manager is very well aware of the threat
  - Secures what he can



# Results

- All but one emerging development was seriously compromised
- Information valued in the billions of dollars
- Pending litigation posture compromised
- Patent applications compromised
- What else is there to say

# Believe it or Not

- *Critical compromises accomplished within one and a half days*
- *No reports of any activities*
- They have much better than average security
  - Technical Security
  - Physical Security

# Remember Risk

$$\text{Risk} = \left( \frac{\text{Threat} * \text{Vulnerability}}{\text{Countermeasures}} \right) * \text{Value}$$

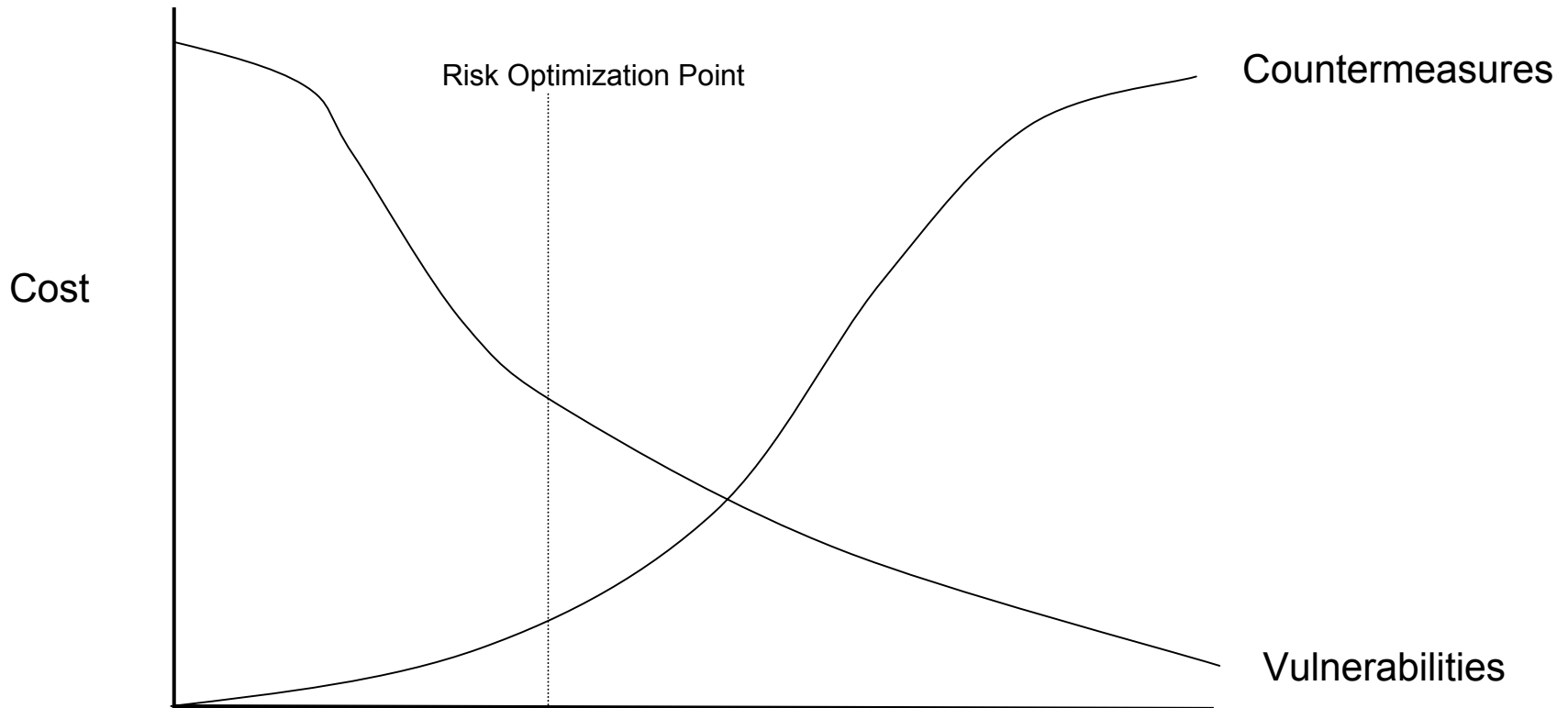
# Threat and Decisions

- The Vulnerabilities exploited were all preventable
- People are however fascinated by Threat
- It only takes bad intent to accomplish what was demonstrated
  - True for any attack
- Stop treating the bad guys as celebrities

# What is a Spy's Security Program?

- The implementation of Countermeasures
- Spies determine the Vulnerabilities that will most likely be exploited
- They then implement Countermeasures to mitigate the Vulnerabilities
- Defense in Depth

# Optimizing Risk



# Potential Loss Should Drive Budget

- Most security programs are determined by money available
  - Risk is a result, not a consideration
- Security program budgets should be a factor of Optimized Risk
  - Risk is the driver for the budget
- Remember, there is a great deal of ROI for most Countermeasures
  - There are only two ways to hack a computer

# Why is Bristow the Worst Spy?

- She runs into good security programs
- She runs into redundant security measures
- The Countermeasures catch her
- She is not a real spy to begin with
- *Alias* actually demonstrates good security programs

# Make Bad Movies

- The reason they are bad spies is because the producers want “good” movies
- They have to have dramatic tension
- Defense in Depth accomplishes this
- They want intrigue and sex
- I’m still waiting for that myself

# Awareness Training

- Awareness
- Awareness
- Awareness
- Awareness

# Summary

- The real spies are sadly better than Bond and Bristow
- Countermeasures should not result from budgets and vendor hype
- Information and services focus, not computer focus
- There should be Defense in Depth
- You must focus on Countermeasures that mitigate Vulnerabilities
- Realistic security is achievable
  - Just look at Bristow and Bond



# For Questions

Ira Winkler

[iwinkler@csc.com](mailto:iwinkler@csc.com)

+1-410-544-3435



EXPERIENCE. RESULTS.