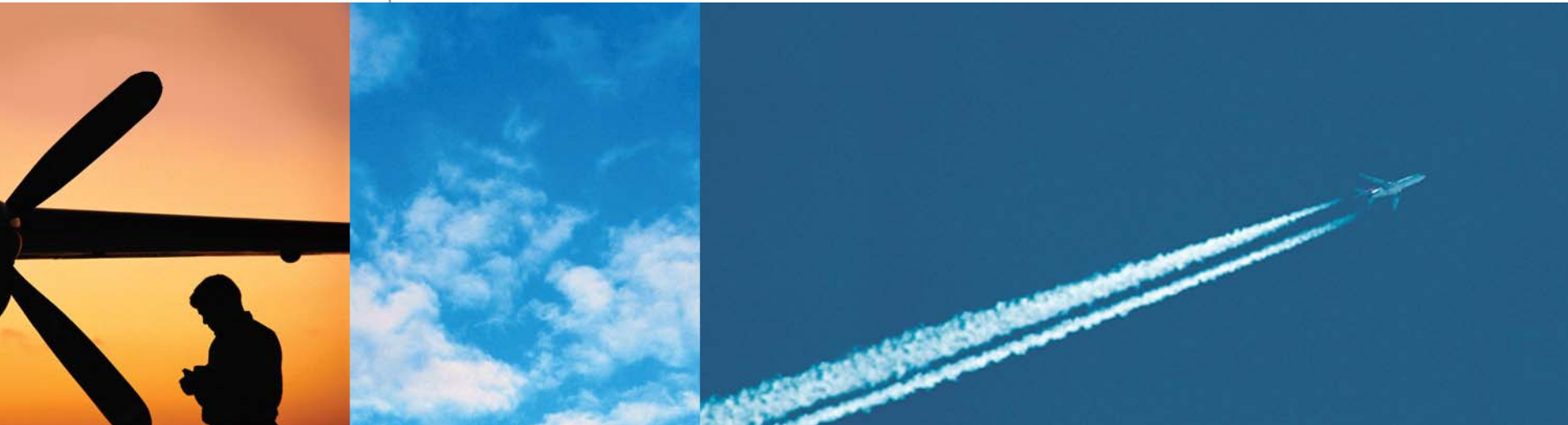


Zen and the Art of Cybersecurity

Ira Winkler, CISSP, CISM

+1-410-544-3435

iwinkler@csc.com



EXPERIENCE. RESULTS.

This is not a Religious Talk

- It is a takeoff of the title “Zen and the Art of Motorcycle Maintenance”
- Through my experience I have learned that the biggest problem with security programs is a false sense of knowledge

Art vs. Science

- If you can describe it and repeat it, it is a science
- People who claim to be “artists” are not
- You want a scientist who can define the process below the art and was trained
 - They truly understand
- There are some people with better abilities and more experience though

Zen of Cybersecurity

People don't know what they don't
know about Cybersecurity

If You Have to Ask, You Shouldn't be Asking

- Too many people ask, “Now that I have work, tell me what I should be doing.”
- Consulting firms get the work, and they sometimes don't have trained people to do the work. Or internal charging methods mean they don't want to use the trained consultants
- It is OK to ask what the current preferred tools are, but again this means they are out of touch with the people who do the work on a regular basis.

The Wrong Perception

- Security is complicated
- Security is expensive
- There is a lack of qualified people
- The qualified people know everything about security
- Of course I am secure, I don't have any problems

Examples of the Real Problem

- 1988 – Morris Worm
- 1991 – AT&T Crash
- mid 1990s – Eligible Receivers
- 1997 – “Banks lose billions of dollars” – PCCIP
- 1997 – Worcester Airport taken down
- 1998 (?) – Power grid crash
- 1999 – Solar Sunrise
- 2000 – DDOS attacks
- 2001 – Code Red, Nimda
- 1990s-Present – GAO reports
- 2003 – Slammer, Blaster
- 2004 - Sasser

More Zen

- What makes a master is an understanding of the basics, and seeing simplicity in difficulty
- You can train and evolve people in the basics
- There are only two (2) ways to hack computers
 - Taking advantage of configuration problems
 - Taking advantage of problems built into software

Security Problems ARE Preventable

- Security should be common sense
- There is no common sense without common knowledge
- Security is a process of correctly maintaining and administering computer systems and people

Automobile Analogy

- Drive safely
- Change oil and other preventative maintenance
- Lock the doors
- Wear seatbelts
- Choose safe routes

- Why don't people do this with security??

The Foundation of Security

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

A Review of IRM

- This is where the concept of a CIO originated
- Computers are basically worthless
- It is the information on, and services provided by, computers that have value
- Although computer security is looked at as a computer issue

Zen and Threat

- When you don't understand your enemy, they seem like geniuses
- Teenagers want significance, and don't need knowledge since you leave yourself open
- Laws won't stop the threat, but just punish them (which is important)

Knights and Dragons

- You need a great enemy to be perceived as a great hero
- A great enemy excuses great incompetence
- Great heroes need lots of money

Fear

- People use fear to
 - Control
 - Scare
 - Get money
 - Get power
 - Fake expertise
 - Deflect blame

Choosing Countermeasures

- How it is usually done
Threat -> Countermeasures
- How you should do it
Vulnerabilities -> Countermeasures
- Government is an exception in some cases

Remember

- Countermeasures are independent of Threats
- Countermeasures that stop terrorists, stop script kiddies
- Just figure out how to phrase what you want in a way management wants to hear it

Right Experts at the Right Time

- A transmission expert may not be an engine expert
- Security experts think they know more than they do about subjects outside their expertise
- Security seems like a single discipline, but it is multiple disciplines
 - Policies, assessment, architecture, encryption, system security, etc.

Cyberterrorism is not Effective

- The goal of terrorism is to create terror, NOT DAMAGE
- Nimda or Anthrax?
- Terrorists want visual attacks
 - TWA 847, Pan Am 103, Oklahoma City, World Trade Center, Pentagon
- Attacking computers doesn't create that terror, but effectively enables attacks

Physical Attacks are Infinitely More Effective

- Hacking a generator can take it down for a week. Blowing it up is easier and will take years to recover from.
- Resources are permanently denied
- Physical attacks create more fear and confusion
- Physical attacks are visual

Death by 1,000 Cuts*

- While people worry about “Spectacular Attacks” they ignore the little losses
- The little losses add to billions of dollars in lost productivity and other resources
- Nimda was a minor concern but cost companies \$1,000,000,000 even though it was not terrorist related
- The little things cost billions

* - Credit to Bill Boni

Security Culture

- Security is a management problem
- Security is a process not a technology
- Management focus drives the effectiveness of your security company
- What type of company are you?
 - Should you be secure, or must you be secure?

What Type are You?

Type I

Type II

Type III

CEO thinks security is a SHOULD	CEO thinks security is a SHOULD	CEO believes security is a MUST
CIO thinks security is a SHOULD	CIO believes security is a MUST	CIO believes security is a MUST

Disaster follows
CIO takes fall

Significant losses
CIO covered

Some losses
Cost savings

Remember IRM

Are you budgeting security based on computer value or information and services value?

What Will Work

- Wizard of Oz approach
- Focus on the basics – NOT THE HYPE
- Decide on the countermeasures that address the most common vulnerabilities
- Training of current workers
 - Let them know what they don't know!
- If you don't do the basics right, nothing else will make a difference

Security Should Be Built in, Not Bolted On

- Are security people involved from the start of projects?
- Are you relying on people in other disciplines to incorporate security because, “they do it all the time”?
- Think of a car with Bolted on Security

For More Information

Ira Winkler, CISSP

iwinkler@csc.com

+1-410-544-3435