

# Making The Most Of Your Opportunities With Management

Stephen Northcutt  
*SANS Institute*

## Executive Summary

This talk is the result of mistakes I have made.

Some of the most promising technical initiatives I have worked on died because I failed to get support or funding from management.

I learned that my technical career could flourish or be hampered by how well I interacted with management.

2

**My hope when I designed this course was that each of you would learn, or remember, a couple of things that we cover and apply those in your daily life.**

**Before there was POP story.** In 1983 - 1984 PCs were rapidly being deployed in the workplace, but their networking was rudimentary at best. Email was still mostly done as a terminal application on a minicomputer. Mini computer disk space was very pricey at the time and we observed that PC XT's had **huge** 20Mb disks. What if we could make it easy for users to upload and download their email from the minicomputer? They could do their work on the PC! And, if we could write/find a version of uuencode for DOS, they could even mail their WordPerfect files as attachments. It would be as nice as a minicomputer based office automation suite, which we had and for a princely sum.

There was a guy at a university somewhere who had posted some code that was a forerunner of POP. We got it, got it ported, (this was before ./Configure), and wrote the PC "glue" software. Weeks later we demo'd it. The response, "**why would anyone want that?**" What happened?

## Game Plan

C  
ommunication

P  
ower

C  
onflict

R  
eaction

P  
ersistence

3

Looking back, I understand that we failed across a number of dimensions of basic human interaction. We didn't **communicate** what we were doing well in advance in bite size chunks; instead we hit them all at once with our spiffy demo and made their eyes glaze over. We didn't take into account there would be a **power** encounter. The mini computer email czar liked buying and controlling expensive disk space. Her motto was, there is no problem on earth so great I can't fix it with a disk quota. The project might have survived anyway, but she was able to cast the issue as a personality **conflict**, not a technological breakthrough. We failed to get management to **react**. We were talking about a potential savings of millions of dollars, but instead of showing the metrics that indicated we were looking at first year savings of \$150K/month, we just said, you will save a lot of money and figured it was their job to count the beans. Finally, when they ignored our spiffy code, we were so disheartened we gave up. We had not yet adopted the discipline of **persistence**.

Later in life, when the US Navy was trying to terminate the Shadow Intrusion Detection project, **persistence** above all else, helped us to survive so that Shadow is the IDS of choice at many high security government locations.

# Communication

4

## Communication

- There is more to communication than Rx and Tx inputs.
- Some protocols are more effective than others.
- Written, distributed information has more authority than interactive conversation.

5

### **DITSCAP process poster story**

I work in Washington DC these days. I am a technical person with a strong security background, and consider myself literate. I've authored books on security and read many more. I have never seen an accurate network wiring diagram I couldn't follow, and some of those get pretty hairy. I was in an army facility recently and they had a poster on the wall. It must of have been a six foot long illustration of the DITSCAP process and the longer I stared at it, the less I understood. They clearly made no effort whatsoever to make the information attainable by the average Joe. They were speaking their own protocol with no concern that anyone else outside of their inborn clique could understand the material.



## Listen Listen Learn Learn

Listen to people when they talk;  
Write down their questions and comments.

Be willing to say "I don't know", ( they  
would soon find that out anyway).

6

**Kairos motto** I spend some time in maximum security prisons in a Christian reach out ministry called Kairos. The night when we first meet the inmates is really interesting; these are some rough characters. But they come, and relationships are formed. They just want to be listened to; everybody wants to be listened to.



## Speaking: Simplify, Clarify

Does it drive you crazy when someone drones on and on with no point?

Prepare to speak. Have a point.

Make the effort to have a word picture, a chart, a jingle, something to help your audience understand and remember what you convey.

7

**Charlie Brown in school**

**A little security is better than less security story**

## The e-medium is *not* the message

Email is not the only communication method:

Three messages and a phone call

Three phone calls and a meeting

8

Computer people are often introverts. I used to say they are more comfortable communicating by email, but as time goes on I meet more and more computer people who don't even do that.

Email "conversations" tend to get corrupted; you need to back them up with phone calls. There is a limit to what you can do with phone calls; meeting someone face to face doesn't really hurt *that* much!

Flame on may work in comic books, but it is a bad idea in the work place.

## Responding to e-mail

- If you read something in email that troubles you, pick up the phone, make an appointment; go over to the manager's office. Be responsive.
- Your email response should be the same order of magnitude as the initial message. A paragraph shouldn't invoke a novel.

9

In general, if you find that you have been composing the same mail message for over an hour, then you probably shouldn't send it.

## Power of the Written Word: email

For all e-mail's risks and faults, having a written audit trail can be very useful.

10

### EMAIL Story

I had been working on this project to help a site move from a situation where everyone ran their own mail servers to a corporate mail server in preparation for a more firewalled environment. This one guy from networks just kept giving me trouble. He was very uncooperative and was slowing the program down at every turn. I had kept all the email, all the promises, all the disrespectful statements. Finally, we had the "show down" meeting. He started by saying, "You've got me and I know you've got me and that makes me really mad".

## Power of the written word: web

Having information, policy, recommendations on tap with an INTRANET page is a good thing™.

If someone asks *"is it documented anywhere?"*, and you can toss them a URL, you have a big win.

11

### **Wayne and Dianne Story**

I was working for a Navy facility trying to help them improve their overall information protection architecture. One of the things I tried to implement there was a commonID system.

So, I told the corporate information systems folks this was the procedure, and they pitched a hissy fit. We aren't going to do that; it is too hard to make sure folks have a commonID. That really surprised me. It seemed pretty durned easy; we even had a database query screen. So I kept arguing the merits of the approach. They weren't buying it. Then at one point, when the conversation was really hot, they asked, "where is this policy documented?". Well, I love policy, I love distributing policy, not big stupid policy, but short, clearly written policy, so I showed them. They chilled right out. It was like pouring oil on water. Calm. Many people rank what is written above what is reasonable.

## A gram of metrics is worth a pound of opinions

- Collect supporting data from vulnerability studies, intrusion attempts, syslogs, firewall logs....
- Turn the data into charts and graphs.
- Display them on your web page, refer to them often.
- Some people learn better from text, others from pictures; meet their needs.

12

### The CONOPS story

**A retired “behind enemy lines intelligence type” and I were asked to develop a pragmatic, deployable approach to offensive information warfare. After years of being on defense, that was a fun twist. Then we presented it to the guy who asked for it. He started off the meeting by saying, “I haven’t looked at it, tell me about it”. Then he shot at everything we had to say. But we had our ducks in a row; we had done our homework. We had synthesized my technical and defensive experience with my partner’s tradecraft. We had facts, we had charts, we had studies, we tag teamed like crazy, and won the guy over.**

## Structureless meetings considered harmful

- If you call a meeting, have an agenda
- If you didn't call the meeting, be prepared with an agenda, briefs
- Take notes, distribute them, (laptops are good, but some people apparently consider them "rude")
- Don't leave a meeting without SMART objectives

13

### **Action item list story**

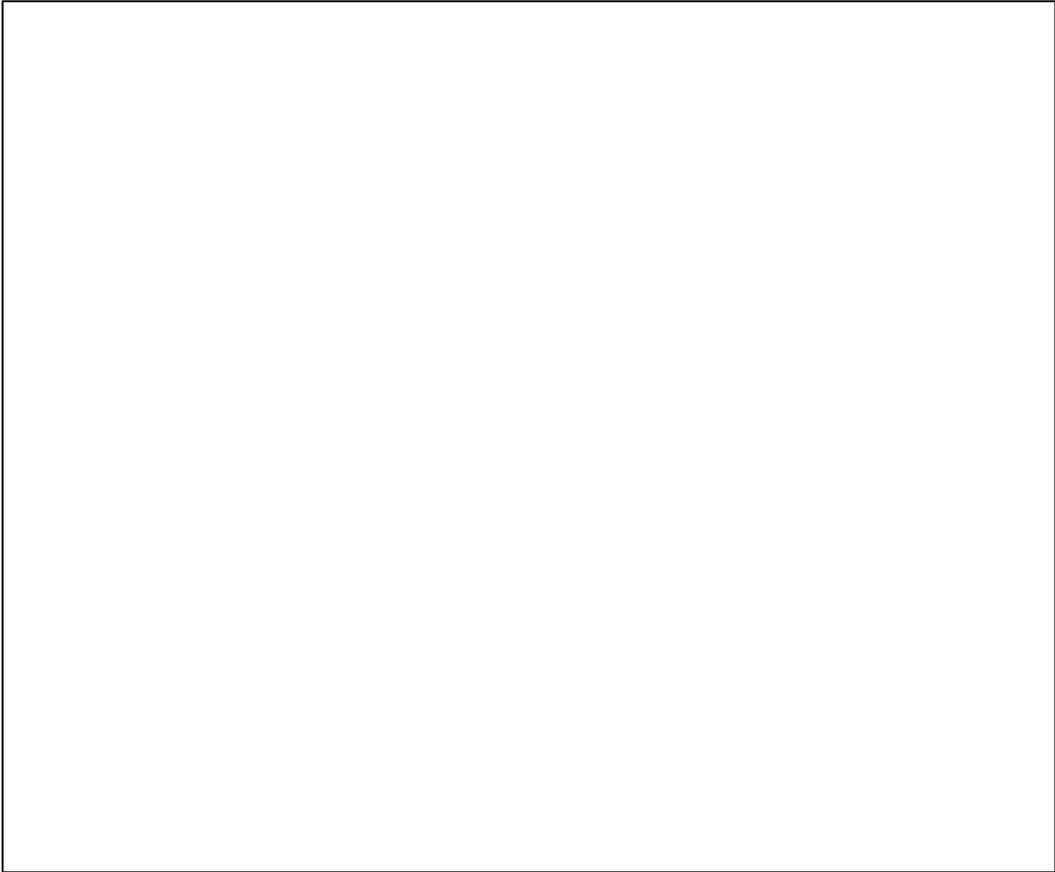
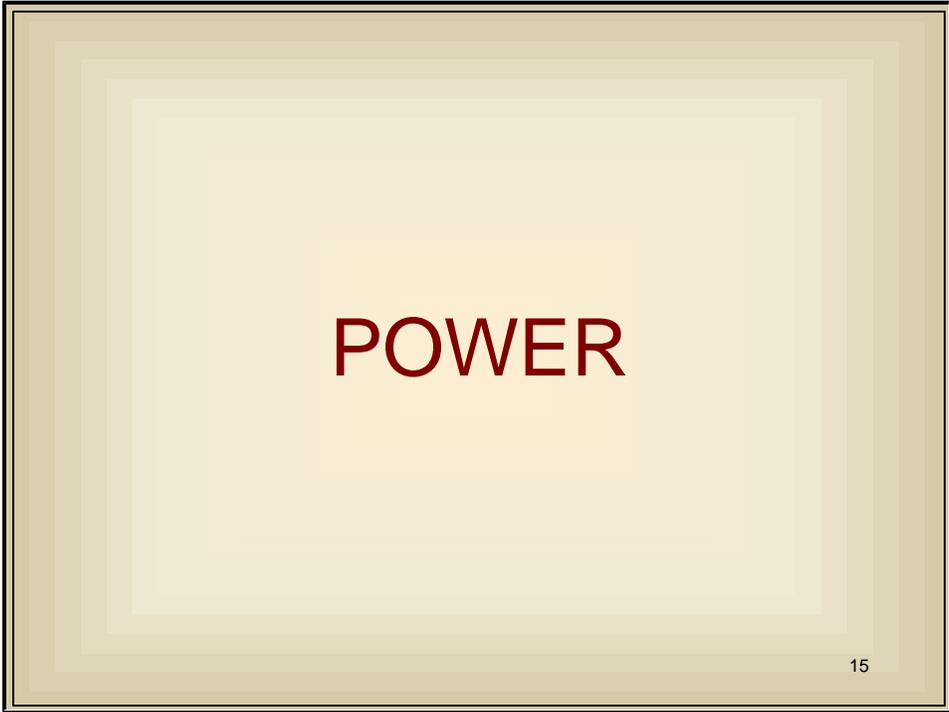
I was in a group once that had weekly meetings, but no one was tracking action items. I am always willing to serve as the recorder, after all the power of the pen is something I never want wielded against me. After a few weeks it was obvious the items weren't getting done, several folks in the meeting asked that we quit tracking the action items. I suggested that we move to a monthly meeting if we could meet weekly deadlines.

One of the symptoms of a dysfunctional organization is meetings where nothing gets accomplished. If you want to be effective you have to assign action items.

# SMART

**S**pecific  
**M**easurable  
**A**chievable  
**R**ealistic  
**T**ime based

14



## The Power Problem

- Management hires and fires
- Management does evaluations
- Management has a lot of power over technical people
- Technical people often need to be careful of speaking too candidly

16

**Anyone ever been screwed out of a well deserved bonus or rating by a pointy haired boss?**

One can say management is clueless, but we can't say they are powerless to affect our career and opportunities.

## The Power Problem (2)

- Technical people write software and build systems
- Technical people can have a profound effect on the corporate infrastructure
- Management tends to be a little uneasy about the power technical people wield

17

### **Wizard observation**

The best technical people are often referred to as wizards. Yet a company can't base its bottom line on magic. So it may be an ego boost to be considered a wizard whose ways are subtle, and is quick to anger, but it doesn't usually result in more trust or opportunities.

## The Power Problem (3)

- Both sides tend to be a little uneasy
- Nobody wants to appear ignorant
- Because they are uneasy, both sides want to show off their expertise

18

### Briefing Don

I have had some great bosses, but I did work in a Dilbert cartoon at one point. I would get an assignment, go in to brief the boss, get through three, maybe four slides. He would ask some questions, make some comments and then suddenly he would say something like: **“I’m not sure this fits into the big picture, how does this relate to the corporate strategic plan”**? I was so freaked out; he assigned me to do the project, shouldn’t he know how it fit into the strategic plan????

I was getting pretty frustrated. It was a great job and I was loving life as a principal investigator, or I would have quit in a heartbeat. Then one day it hit me; I was missing the boat. What was actually happening is I was losing him as soon as the presentation got technical. He didn’t want to be caught ignorant, so he was changing the playing field, moving it to management speak. This was something I didn’t understand, so I was feeling ignorant. From then on, I changed my approach. I went to three-slide briefs:

1 A People slide: who is working on the project

2 A Buzzword slide: what we are doing

3 A Directions and Issues slide: when we will deliver what and any major problems.

## The Power Solution: Trust

- Never misuse,(or give the appearance of misusing), the knowledge you have
- Work to minimize the loss to your employer should you leave
- Build backup systems at least two levels deep
- Think problems through steps ahead

19

Maximize what you have in common with management, minimize the difference. You are both paid by and invest some of the best years of your life in the same organization. Make it work! Thank you!

The fact that someone does not have your exact skill set does not make them any less valuable to your organization.

20

**Human resources staff**

## Leading By Serving

- Informed people make informed decisions. If you find you have skills that are important to your organization, and very few people possess them: teach.
- We started a "How Things Work" series on basic network and computer technology as well as classes in our areas of expertise.

21

One of our goals should be to continue to train people to replace us. That may not sound wise in terms of job security. In fact, it does backfire from time to time. However, we can miss a promotion opportunity if there is no one to replace us.

Knowledge is power.

Being misunderstood  
is power misdirected.

22

**If you don't believe knowledge is power, try running a content sniffer for a couple weeks focused on you worst enemy..**

## So Misunderstood

- If you don't understand ::= I am wrong
- At best, if management doesn't understand the issue, they can't fully support us
- If I can't explain something to a five year old ... I can't explain it at all ... outside of my peer group

23

### **Story: I don't understand so you're wrong**

This was another of the “country Kerby” lessons a former boss taught me. His father in law was an astute student of people and when Fred was telling him our troubles, that was his response. When, I first heard it I got really mad, but the more I think about it, the more I think it is correct.

## So Misunderstood(2)

(for any managers in the audience)

Ignorance is NOT a virtue

Don't pretend not to understand as a way  
to avoid or stall on an issue

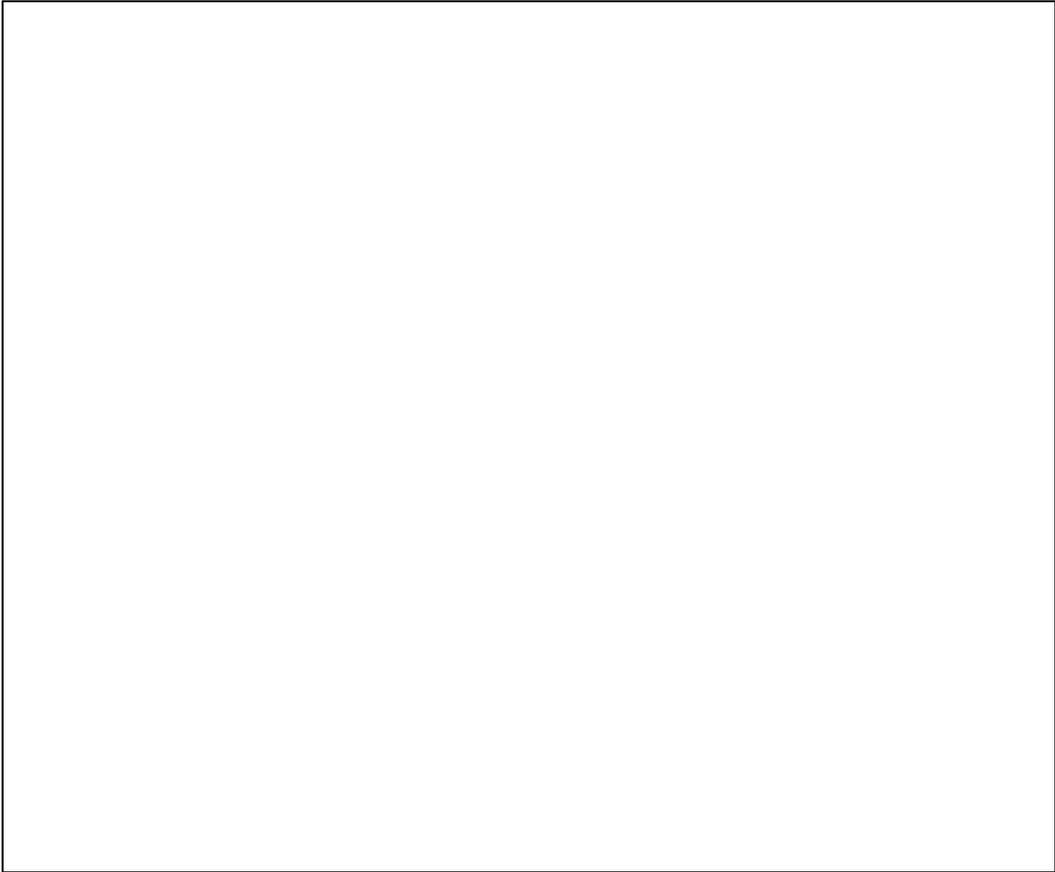
Do your homework, meet us halfway

24

This is the only slide in the presentation directed at managers. You need to keep your side of the bargain.

# CONFLICT

25



Conflict is part of the package

Change always breeds resistance!

26

If you are doing a good job, if you are making progress, conflict has to happen!

**Watosh needs to be responsible for Watosh**

One loud mouthed, thick headed person  
can delay, possibly stop, the best,  
most needed engineering initiative.

**So What?**

27

**SAR school slogan**

This is my codependence slide. You need to be responsible for yourself, and the things you control, nothing else. Do what you can, with what you have, where you are.

## **Solomon doesn't work here anymore**

Put management in a win-win situation as much as possible; try to avoid forcing them to resolve an issue between two warring parties.

28

### **Solomon story.**

The Solomon solution probably wouldn't play well in the Washington Post today. Managers, don't really know the situation and would really prefer that the warring parties come to a resolution among themselves.

## **Don't fight your enemies, retire them**

Keep working to convert your adversaries. As you keep educating people and keep trying to do what needs to be done, you **will** gain support.

29

**Mary story**

## Stroke the underbelly of the beast

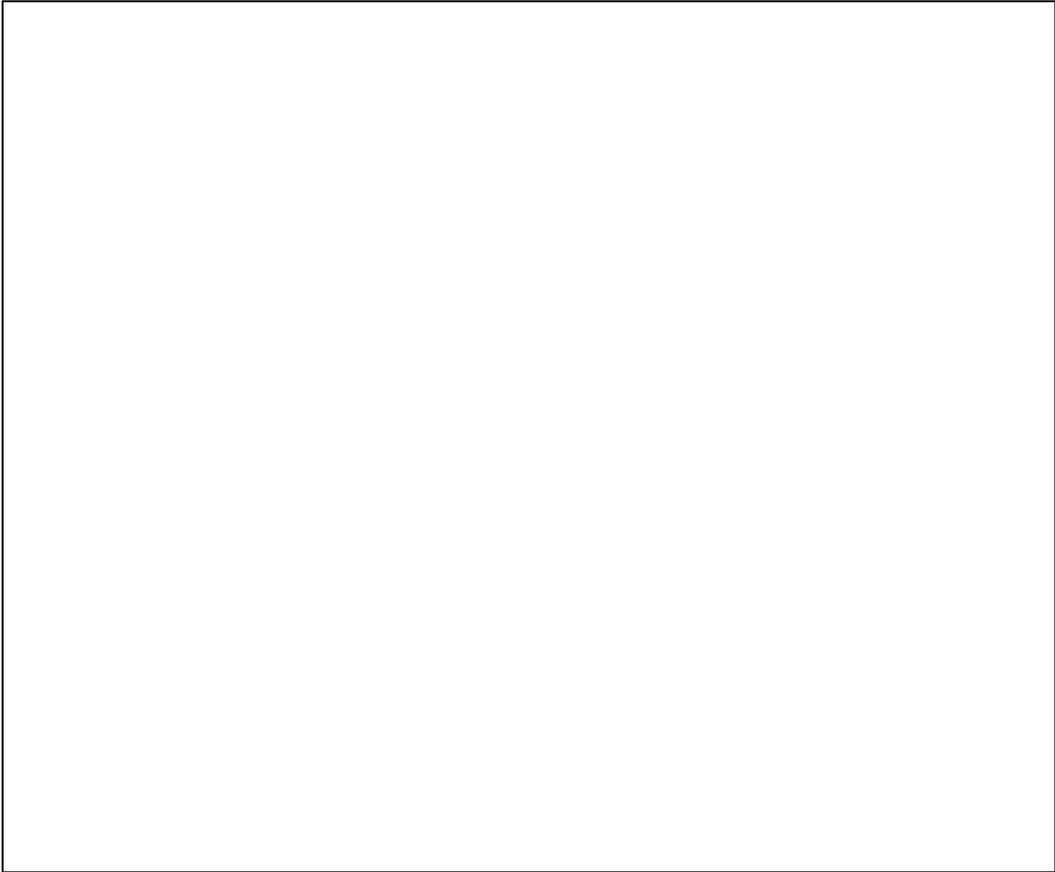
Your worst detractor may have someone on their staff, or may report to someone, sympathetic to your cause.

30

### **Mission Impossible Approach**

Imagine for just a second you were a secret agent and your assignment was to turn an individual, to ensure that he/she became loyal to your cause, or even to make them take a specific action. The only problem is, they hate your organization's guts and everything you stand for; what do you do?

Watch Mission Impossible much? You get to someone close to them, spouse, coworker, secretary, boss and you use that relationship to influence them.



## Incidents as catalysts

If you have been proactive,  
and have planned well, then using an  
incident as impetus to get  
management moving may be good.

Don't go to that well often.

32

### **Continuous Process Improvement by Incident Destabilization Story**

Once a government group didn't get the memo that all Shadow team members were of the rebel alliance and needed to be hunted down and killed. They wanted to see how we accomplished so much with so little money and so few people. Finally, they asked, what about management buyin, how have you gotten your management to support what you are doing across the board. I answered:

One decision at a time using CPI by ID.

What is CPI by ID?

Well, every time there is an incident, the strongest force in the universe, status quo, gets destabilized, albeit for a very short period of time. So every time there is an incident, as soon as I know I can get it under control, but before the incident is close out, I always slip in one improvement, one change.

## Don't forget the reactor rods

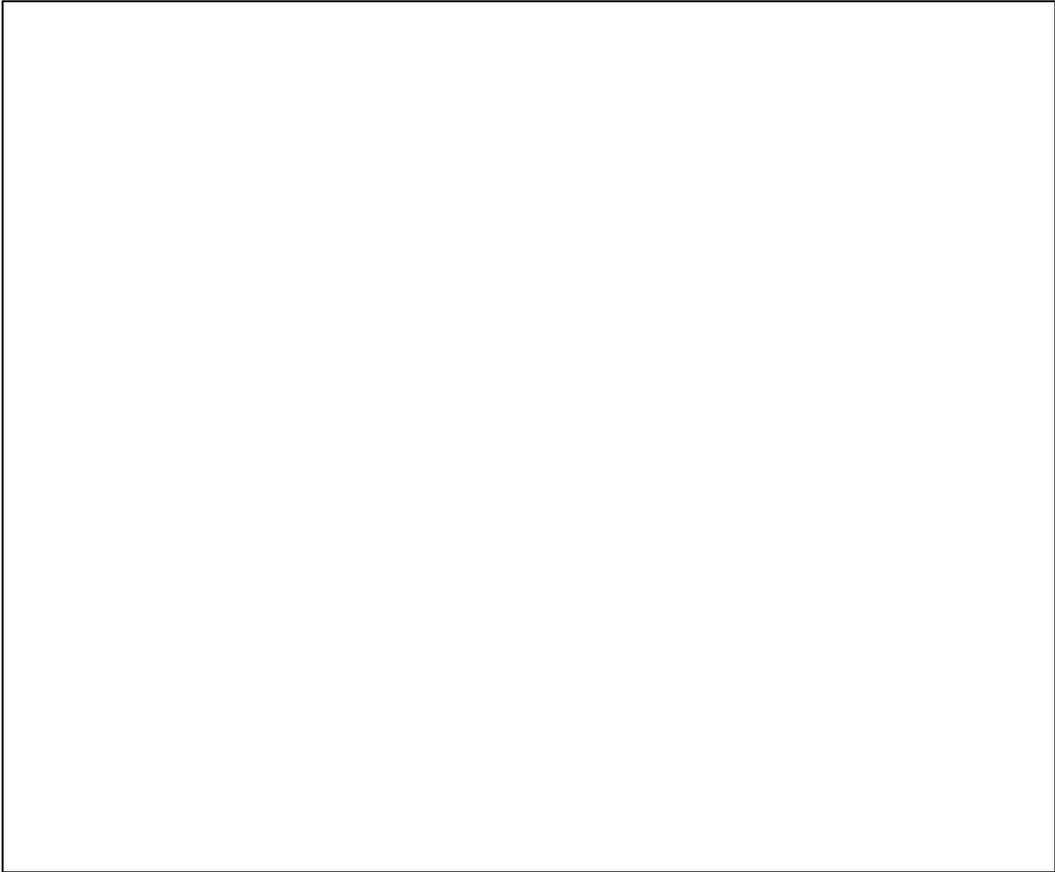
Spinning up senior management may get results, but can have serious side effects. You may get what you ask for; you may get what they think you are asking for; you will almost certainly get more than you bargained for.

33

### **Bullet proof vests story**

# PERSISTENCE

34



## Law of the farm

Stephen Covey points out we reap what we sow. Sow generously, sow often.

35

## Persistence

Plant early, water often.

Ideas that fall flat today may  
bloom six months later.

36

### **Microsoft windows for OA**

A year after my POP adventure, I was assigned to a team to develop alternatives to the Unix minicomputer based office automation system because it was costing too much. I recommended they move to MS Windows and for one reason. Version 2.11 had a primitive round robin multitasking so you could handle a request for information and pick up what you were working on before you were interrupted. However, there were senior managers that didn't back me on the POP approach and they didn't back me on Windows, (these folks went to Macs and ended up having to do a total replacement to get back to the borg, I mean Windows environment, two years later). However, they saw I had a little courage to say what I thought and a little vision and they did back me later.

## Closure is a life style

State the core issues early and often

Stay focused

Seek to move in the direction of closure  
one step at a time

37

### **Story: Sea kayaking expedition**

Life is too short to drift aimlessly. Set a course, stay on course, achieve your destination. Know where you are headed. Know the next step you need to take to get there.

Never compromise your integrity;  
you may not be able to rebuild it.

(Trust is the single most important criteria  
for a security professional.)

38

**The Executive Director authorized it!**

## We Have Covered

Communication

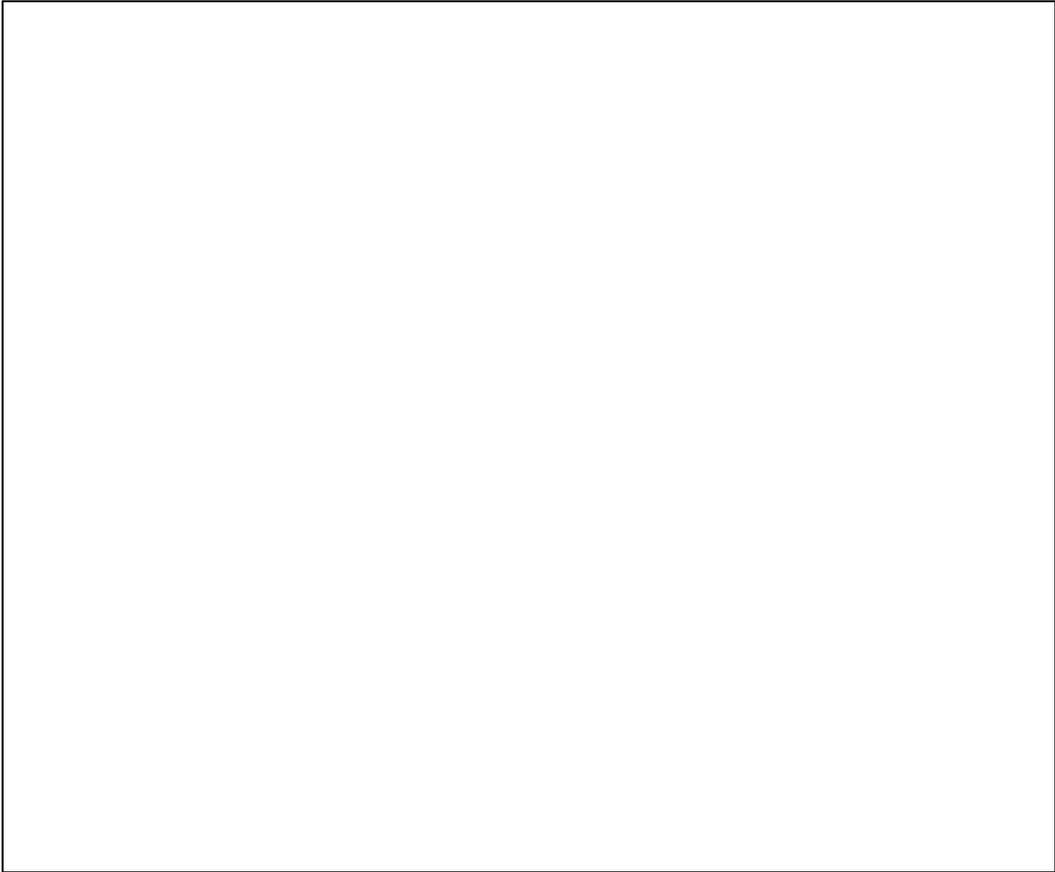
Power

Conflict

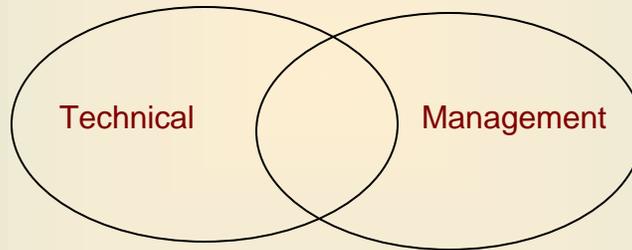
Reaction

Persistence

39



# Conclusion



Different worlds, same goals

40