Physical Security

(You're Doing It Wrong)

A.P. Delchi

WHOIS DELCHI

- Infosec Rasputin
- Defcon, HOPE, Pumpcon, Skytalks
- Minister of Propaganda & Revenge, Attack Research

WHOIS DELCHI

$DIETY

Grant me the serenity to accept people who will not secure their networks,

THE COURAGE TO FACE THEM WHEN THEY BLAME ME FOR THEIR PROBLEMS,

AND THE WISDOM TO GO OUT DRINKING AFTERWARDS

"You're Doing It Wrong"

A phrase meaning that the method you are using is not creating the desired result

Your Mission

Your Mission

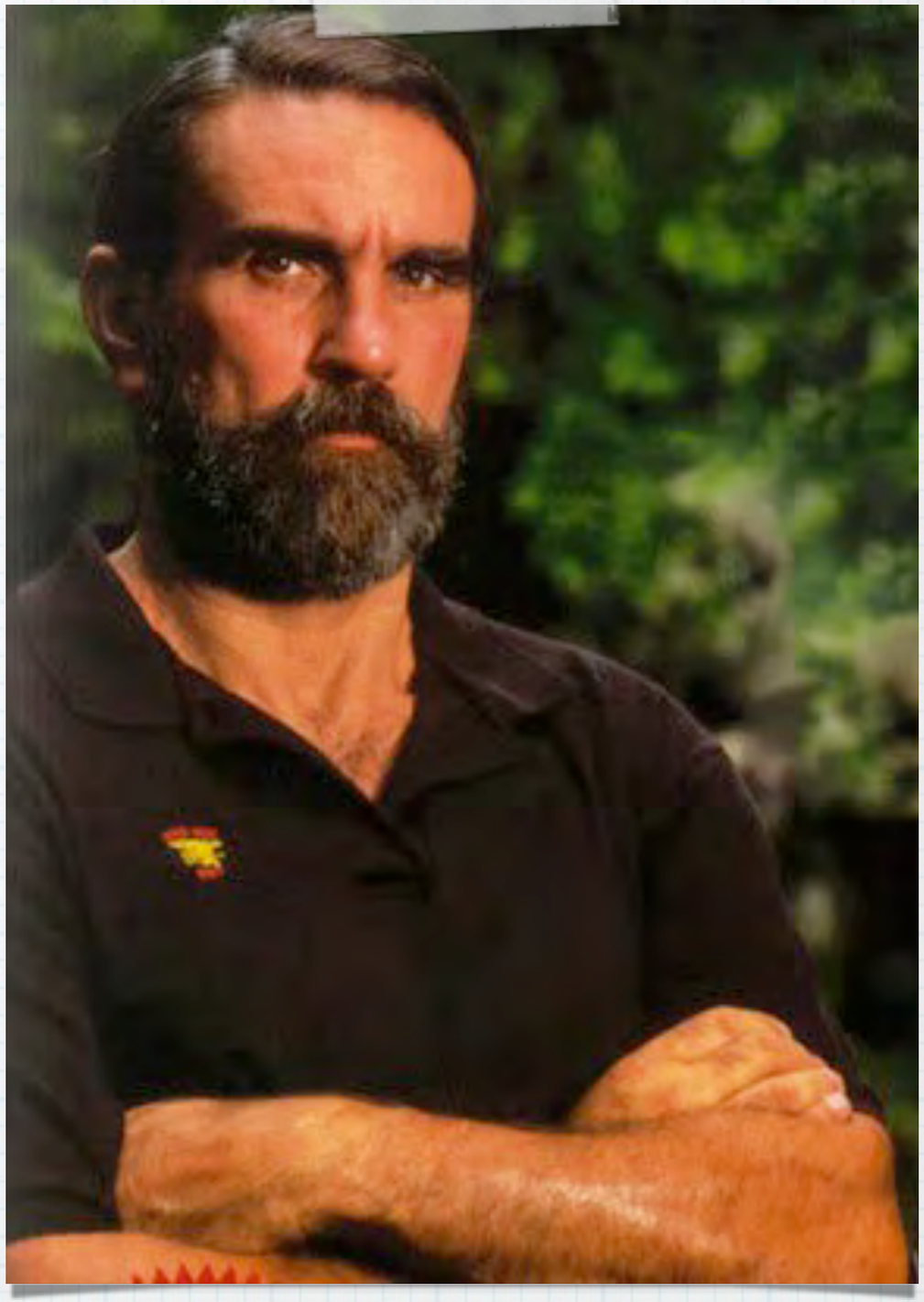
Design and implement a physical security system for a new facility, to include multi-factor authentication and video surveillance.

Saturday, July 3, 2010

“Proper Previous Planning Prevents Piss Poor Performance”

Dick Marcinko,

“The Rogue Warrior”



Physical Security

Physical Security

Physical security describes both measures that prevent or deter attackers from accessing a facility, resource, or information stored on physical media and guidance on how to design structures to resist various hostile acts.
en.wikipedia.org/wiki/Physical_security

Physical Security

Physical security describes both measures that prevent or deter attackers from accessing a facility, resource, or information stored on physical media and guidance on how to design structures to resist various hostile acts.
en.wikipedia.org/wiki/Physical_security

Measures to reasonably ensure that source or special nuclear material will only be used for authorized purposes and to prevent theft or sabotage.
www.nrc.gov/reading-rm/doc-collections/cfr/part110/part110-0002.html

Physical Security

Physical security describes both measures that prevent or deter attackers from accessing a facility, resource, or information stored on physical media and guidance on how to design structures to resist various hostile acts.
en.wikipedia.org/wiki/Physical_security

Measures to reasonably ensure that source or special nuclear material will only be used for authorized purposes and to prevent theft or sabotage.
www.nrc.gov/reading-rm/doc-collections/cfr/part110/part110-0002.html

The measures used to provide physical protection of resources against deliberate and accidental threats.
www.tsl.state.tx.us/ld/pubs/compsecurity/glossary.html

Physical Security

Methodology

- Assessment
- Assignment
- Arrangement
- Approval
- Action

Methodology

assessment

A thorough examination of the facility to be protected.

Methodology

assessment

- Scope of property to be protected
- Established points of entry and egress
- Potential points of entry and egress
- Existing security measures
- Evaluation of physical property
- Risk assessment

Methodology

assignment

Establish the required level of security for specific areas and assets within the facility.

Methodology

assignment

- High level
  - ✓Data Centers
  - ✓Executive Offices
  - ✓Finance & Accounting

- Medium Level
  - ✓ Entry & Egress
  - ✓ Reception
  - ✓ Elevators

- Low Level
  - ✓ Common Areas
  - ✓ Cubicle Farms

Methodology

assignment

- Considerations
  - ✓ Insurance requirements
  - ✓ Compliance requirements
  - ✓ Fire code requirements
  - ✓ Business requirements

Methodology

arrangement

Establish the most effective locations for security devices based on their requirements.

Methodology

arrangement

- Cameras
  - ✓Field of view
  - ✓Redundancy
  - ✓Tracking

- Doorways
  - ✓ Type of locks
  - ✓ Multi factor authentication
  - ✓ Time based restrictions

- Central Control
  - ✓ Cabling limitations
  - ✓ Power, archiving, and disaster planning

Methodology

approval

Submit all plans, costs, schedules and related data to management.

Methodology

Approval

- Hardware
  - ✓Quotes form multiple vendors
  - ✓Lifetime requirements
  - ✓Service plans

- costs
  - ✓ Plan A, B, and C
  - ✓ Flexibility
  - ✓ Options

- Schedule
  - ✓ Time frame for completion
  - ✓ Interference with business operations

Methodology

action

Implementing the physical installation and configuration of the approved system.

Methodology

Action

- Construction
  - ✓Oversee construction
  - ✓Oversee inspections by state / local govt
  - ✓Manage corrections

- Training
  - ✓ Security officers
  - ✓ Users
  - ✓ Establishing policy & procedure

- Testing
  - ✓ Ensuring the system works as planned
  - ✓ Compliance testing

What Could Possibly Go Wrong?

"No plan of operations extends with certainty beyond the first encounter with the enemy's main strength."

Count Helmuth von Moltke

Saturday, July 3, 2010

Methodology

TRAINING METHODOLOGY

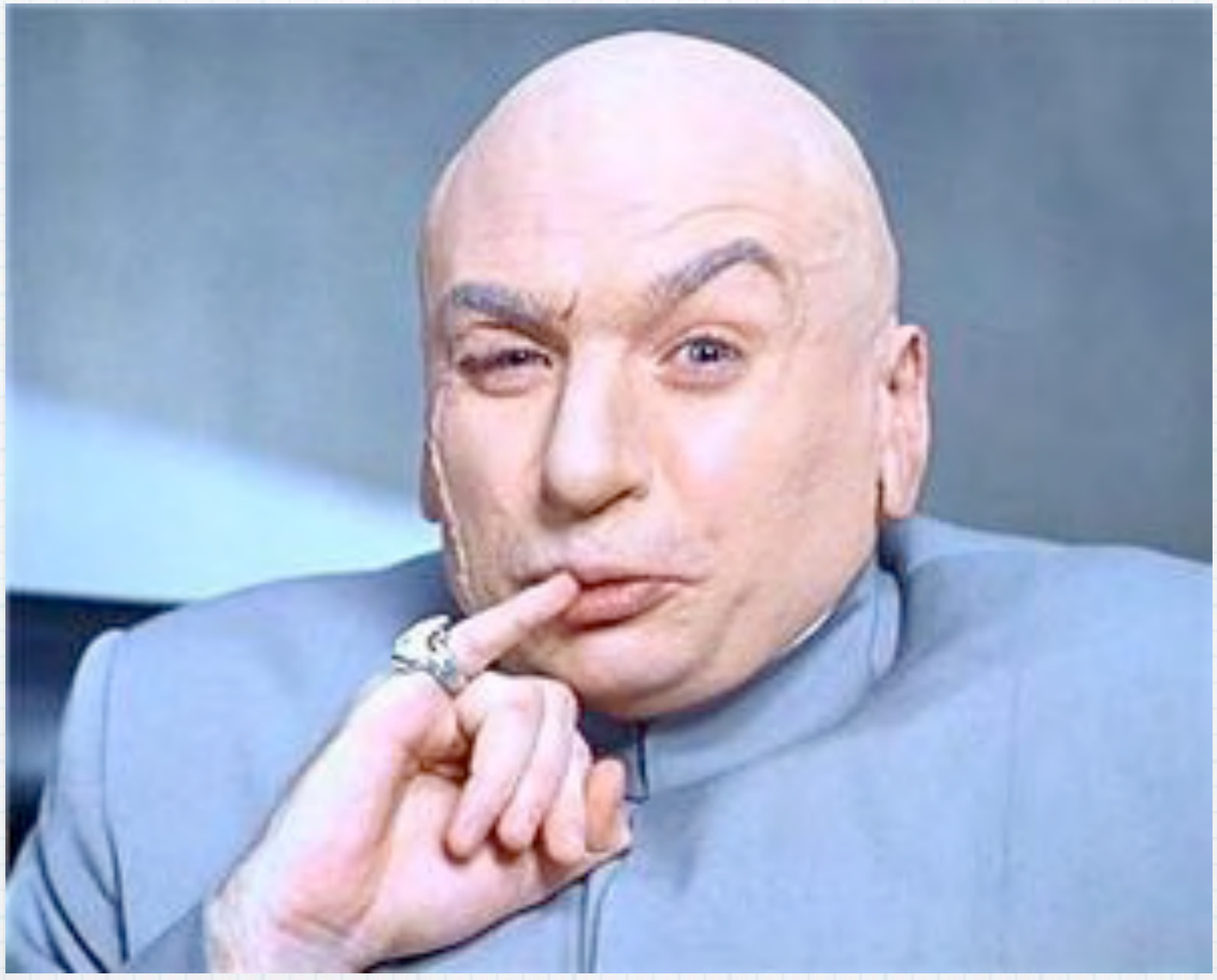
Experience

Training Methodology

Planning Experience

Training Methodology

Saturday, July 3, 2010



Saturday, July 3, 2010

Saturday, July 3, 2010

Management

Management

Management

Pros :

- ✓ Provide Budget
- ✓ Set Requirements
- ✓ Sign your paycheck
- ✓ Run the show

Cons :

- ✓ They know this

Strife

Strife

"I want a state of the art high tech system. FBI, CIA kind of security"

Strife

"I want a state of the art high tech system. FBI, CIA kind of security"

"I can do that. Based on your needs, and the floor plan it will cost $54,875."

Strife

"I want a state of the art high tech system. FBI, CIA kind of security"

"I can do that. Based on your needs, and the floor plan it will cost $54,875."

"Can't you just buy something from Costco?"

Strife

"I want a state of the art high tech system. FBI, CIA kind of security"

"I can do that. Based on your needs, and the floor plan it will cost $54,875."

"Can't you just buy something from Costco?"

<redacted>
CEO of Information Security Firm

≠

Strife

Strife

"I went to Best Buy and saw a HDMI cable for $50. I went home and surfed the internet for a while and found the same cable for $2 from a web site in China. If I can do that for a cable I expect you to do the same thing for my security system."

Strife

"I went to Best Buy and saw a HDMI cable for $50. I went home and surfed the internet for a while and found the same cable for $2 from a web site in China. If I can do that for a cable I expect you to do the same thing for my security system."

<REDACTED>
CEO of Fortune 500 Security Firm

Be knowledgeable on the equipment , methodology and best practices for your industry.

Understand the impact that your project will have on business & user activity

Rely on facts, not speculation , theory, rumors, or maybes.

Present facts, support with documentation, explain risk and impact, prove mitigation

Present in a factual & respectful manner, showing your work and explaining your reasoning behind the design

If you don't know, you don't know. State that you will research and return with the answers

Be prepared to loose gracefully

SUCCESS

SUCCESS

"This is one hell of a security system. Whoever did this knew what the hell they were doing."

SUCCESS

"This is one hell of a security system. Whoever did this knew what the hell they were doing."

<REDACTED>
Visitor,
Friend of CEO of information security firm

"Shut up, get it done, failure is not an option."

Charles Rawls

VP of ass kicking

dorsai Embassy, Earth

Vendors

VENDORS

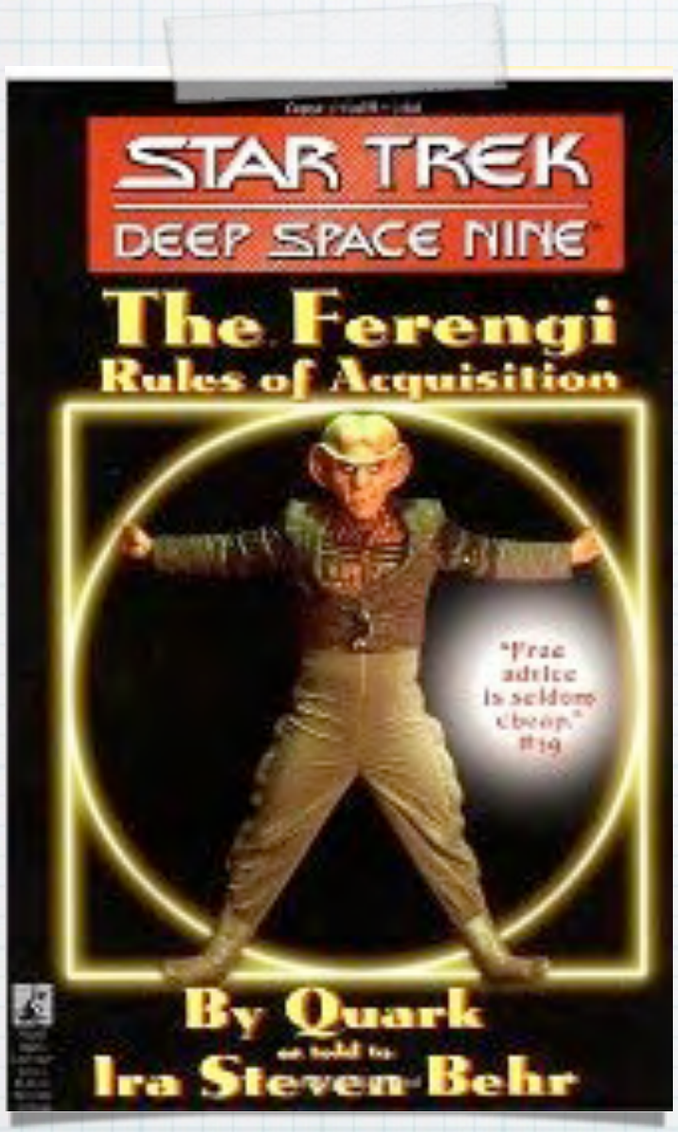
Vendors

Pros :

- ✓ Provide Cool Toys
- ✓ Will Let You Play with The Cool Toys
- ✓ Have historical info on product quality

Cons :

- ✓ Will expect you to buy From Them



"The Ferengi Rules Of Acquisition"

$6.99

ISBN : 0671529366

RULE # 1

There are many , many, many vendors out there

RULE # 2

You do not always need the latest, greatest state of the art item

RULE # 3

Always deal with vendors between 11 AM & 2 PM

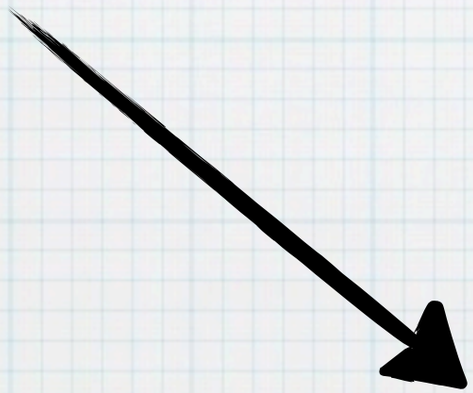
Reality

Reality

Requirements

Reality

Requirements



Reality

Requirements

RFQ

Reality

Requirements

RFQ

Reality

Quote

Requirements

RFQ


Circle Jerks
WITH
SPECIAL GUESTS

Never rely on a single vendor

Do not get caught up in vendor wars

Ensure that the vendor is knowledgeable on the products they are selling

Do your own product research

Beware of unnecessary up-selling

Get details on all aspects ... warranty, service , training ....

Do not be afraid to revise your RFQ

Do not be afraid to READ your RFQ

Keep all paperwork, quotes, and RFQ revisions

Prioritize your needs to make a balance between budget and equipment

Look for hidden costs, cost creep, feature creep, and after contract expenses

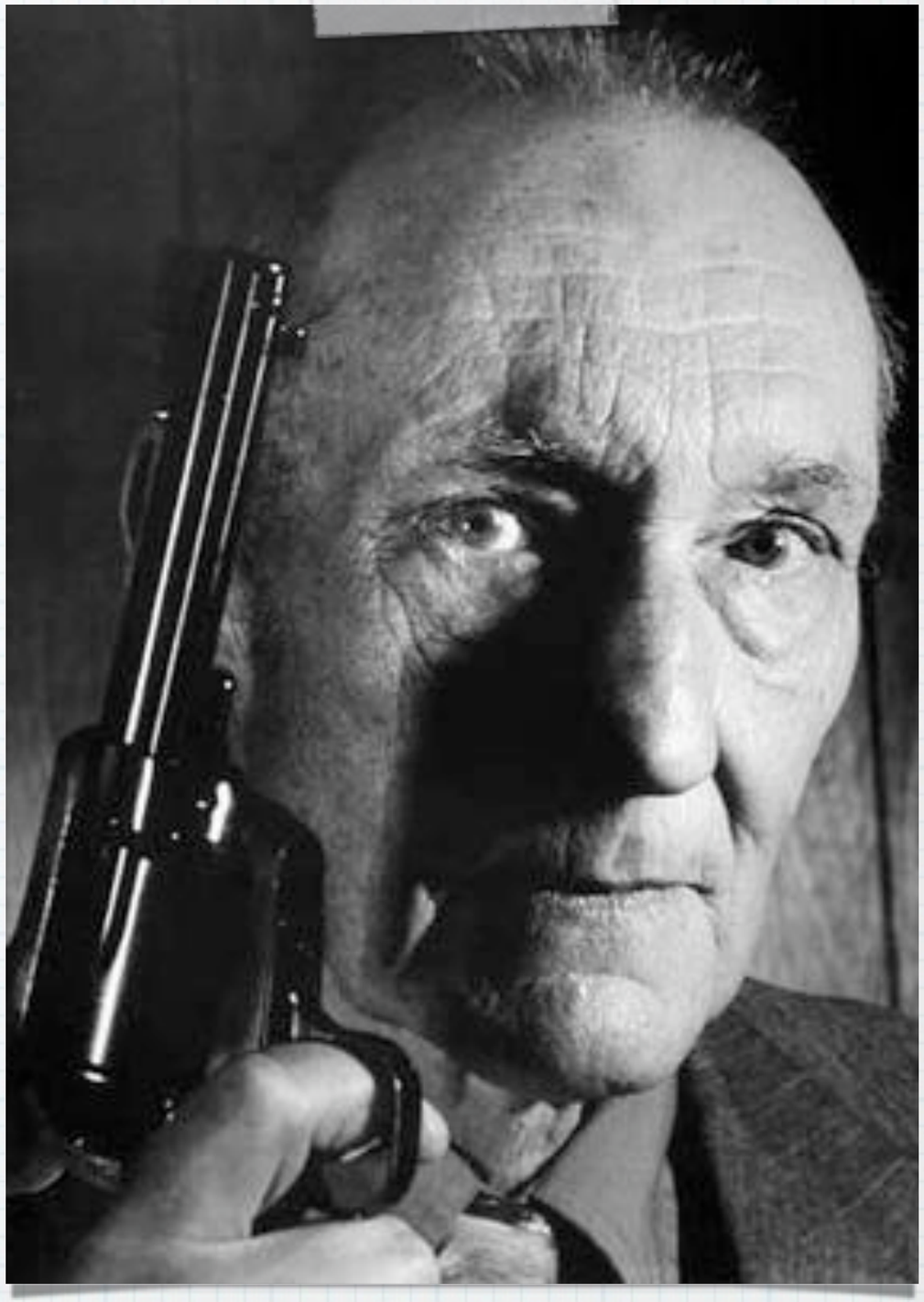
If you work with multiple vendors for components of a system it is YOUR responsibility to ensure that the products will work together

Know up front if sub-contracting will happen, and if so do due diligence on the sub contractors

A high price support contract does not always mean high quality support


SCIENCE I
SCIENCE II
ENVIRONMENT
MISSION OPS
ENGINEERING

"There are no honorable bargains involving exchange of qualitative merchandise like souls. Just quantitative merchandise like time and money."



William S. Burroughs

"Words Of Advice For Young People"

People Who THINK They Know More Than You

People Who THINK They Know More Than You

People Who THINK They Know More Than You

PROS :

- ✓ They Usually Don't
- ✓ Make You Look Good
- ✓ Annoy Management

Cons :

- ✓ Rarely Shut Up

"Of course the alarm says it's 105 degrees. The sensor is on the ceiling, and heat rises. It's 105 up there, but down here where the servers are it's NOWHERE NEAR 105."

<REDACTED>

CEO, MIT MBA,

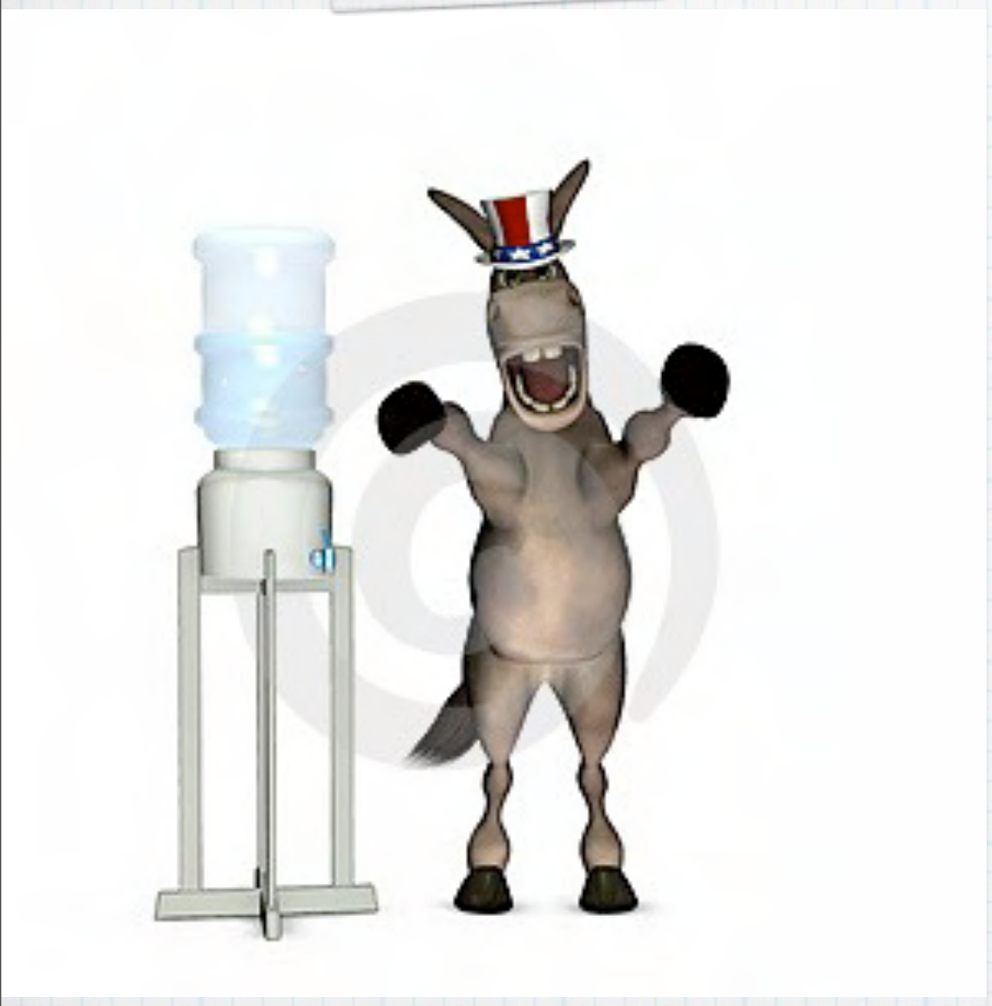
Said 20 Minutes before servers automatically shut down due to thermal alarms

"Of course the alarm says it's 105 degrees. The sensor is on the ceiling, and heat rises. It's 105 up there, but down here where the servers are it's NOWHERE NEAR 105."

<REDACTED>

CEO, MIT MBA,

Said 20 Minutes before servers automatically shut down due to thermal alarms



Know the difference between water cooler talk and factual discourse.

Refute with facts, experience, and a even tone

Do NOT use personal attacks, vulgar insults, or questionable phrases or terms

If they start playing the brownie points game, stop.

If they start playing politics, stop.

If they cite something they heard on AM talk radio, RUN!

Cut sheets from the vendor are a better point of reference than something told to a coworker by their barber who heard it from his cousin who works on the loading dock where the publish that technology magazine .

Do not play buzzword bingo

Know what the terms, acronyms, and technological phrases you use mean.

Let them kiss ass, while you kick ass.

Saturday, July 3, 2010

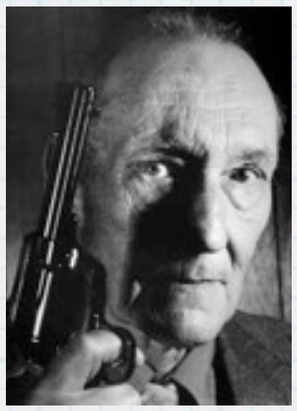
“What about biometrics?”

"What about biometrics?"

"Biometric three phase multi-homed active authentication is the best!"

"What about biometrics?"

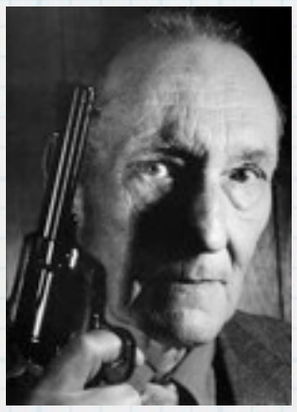
"Biometric three phase multi-homed active authentication is the best!"



"I am not paid to listen to this drivel. You are a terminal fool."

"What about biometrics?"

"Biometric three phase multi-homed active authentication is the best!"



"I am not paid to listen to this drivel. You are a terminal fool."

"*Ahem*"

"What about biometrics?"

"Biometric three phase multi-homed active authentication is the best!"

"*Ahem*"

Saturday, July 3, 2010

“What about biometrics?”

"What about biometrics?"

"Biometric three phase multi-homed active authentication is the best!"

"What about biometrics?"

"Biometric three phase multi-homed active authentication is the best!"

"As per your requirements the RFQ contains two factor authentication with an option for biometrics as a third, pending budgetary constraints. The cut sheets are in your copy of the RFQ."

NO!


i'll spell it MICRO$LOTH WINBLOWS in a DELICIOUS TWIST
i refer to them as NUTSCRAPE and INTERNET EXPLODER, RESPECTIVELY
I CALL IT AO-HELL BECAUSE I'M YET ANOTHER COCKSUCKER

YES!

CONSTRUCTION WORKERS

CONSTRUCTION WORKERS

CONSTRUCTION WORKERS

PROS :

- ✓ Reliable Timing
- ✓ Know Trade Secrets
- ✓ Tell Good Jokes

Cons :

- ✓ Will Do <u>EXACTLY</u> what You Tell Them To Do

Know the work schedule for the construction team

Meet the foreman. Get his contact information.

Read the blueprints.

Read the blueprints again, with the foreman.

Supervise the construction. Look for things that are not quite right.

Expect to find surprises.

Expect to pay to fix them.

Construction workers and their foreman are the first line of defense when it comes to building inspections.

They know what needs to be done, and why.

They deal with the same state/county/city building inspectors on multiple projects.

Listen to them. Do what they say. This is their area of expertise, even if the only adjective they know is “fucking”

“The fucking wiring is not hooked up to the fucking switch correctly, so it’s not going to fucking work. It’s fucked.”

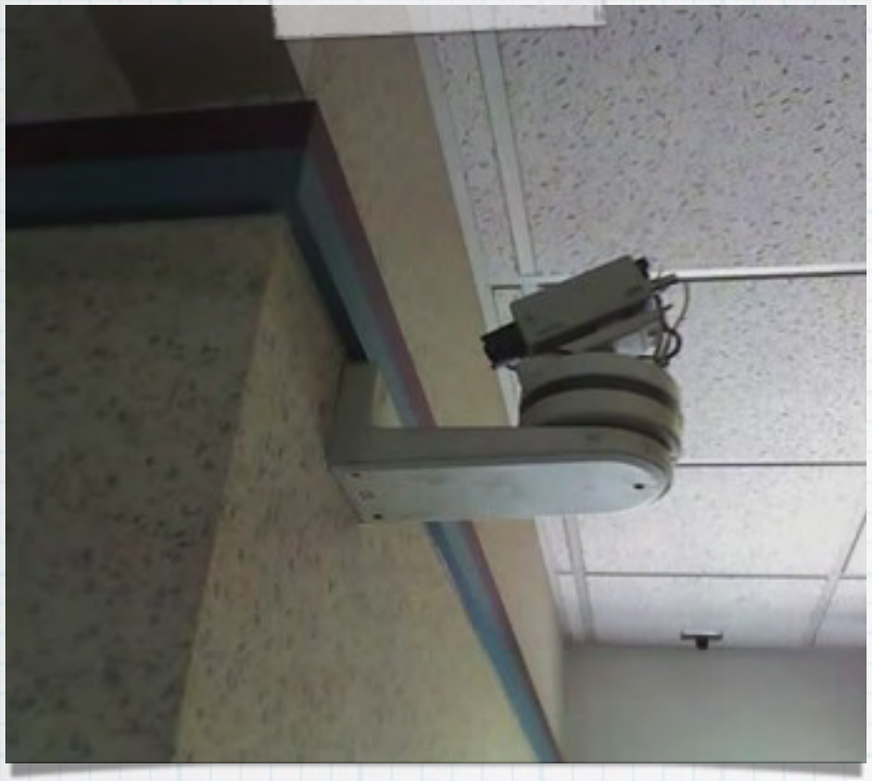
-NJ construction worker

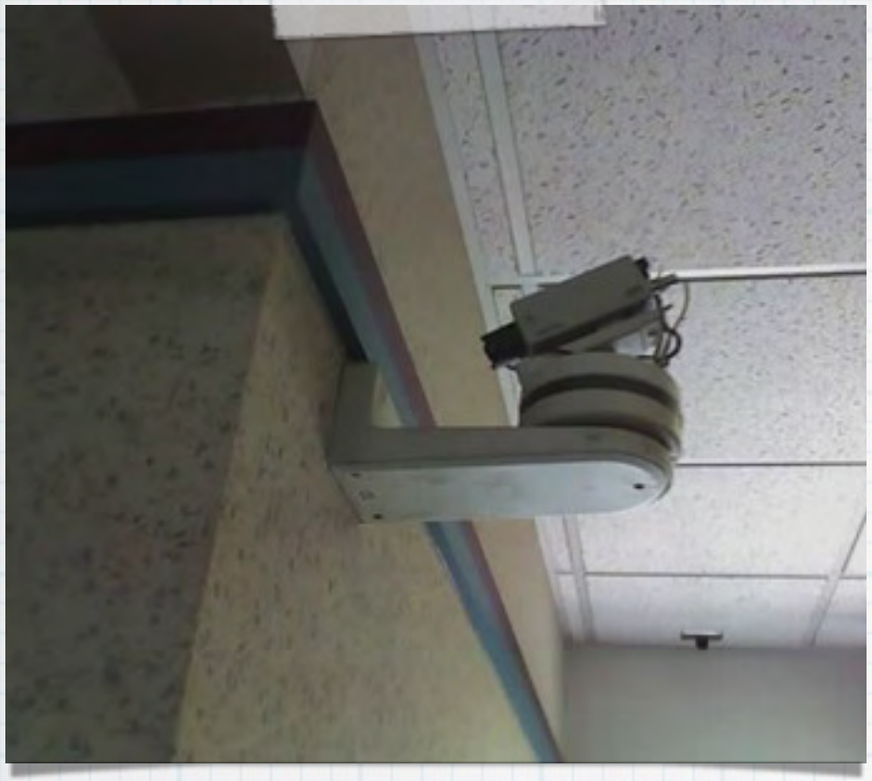
Construction workers on your project may not speak English.

If this is a problem , deal with it before work begins.

Consult with HR before bringing up the subject.

If you can not communicate with each other there is no way to indicate problems, make changes, or share dirty jokes





Things Will Go wrong

Not all problems can be solved with a clever work-around.

A quick fix today can be a problem tomorrow.

Pizza and beer is cheaper than overtime.

USERS

USERS

USERS

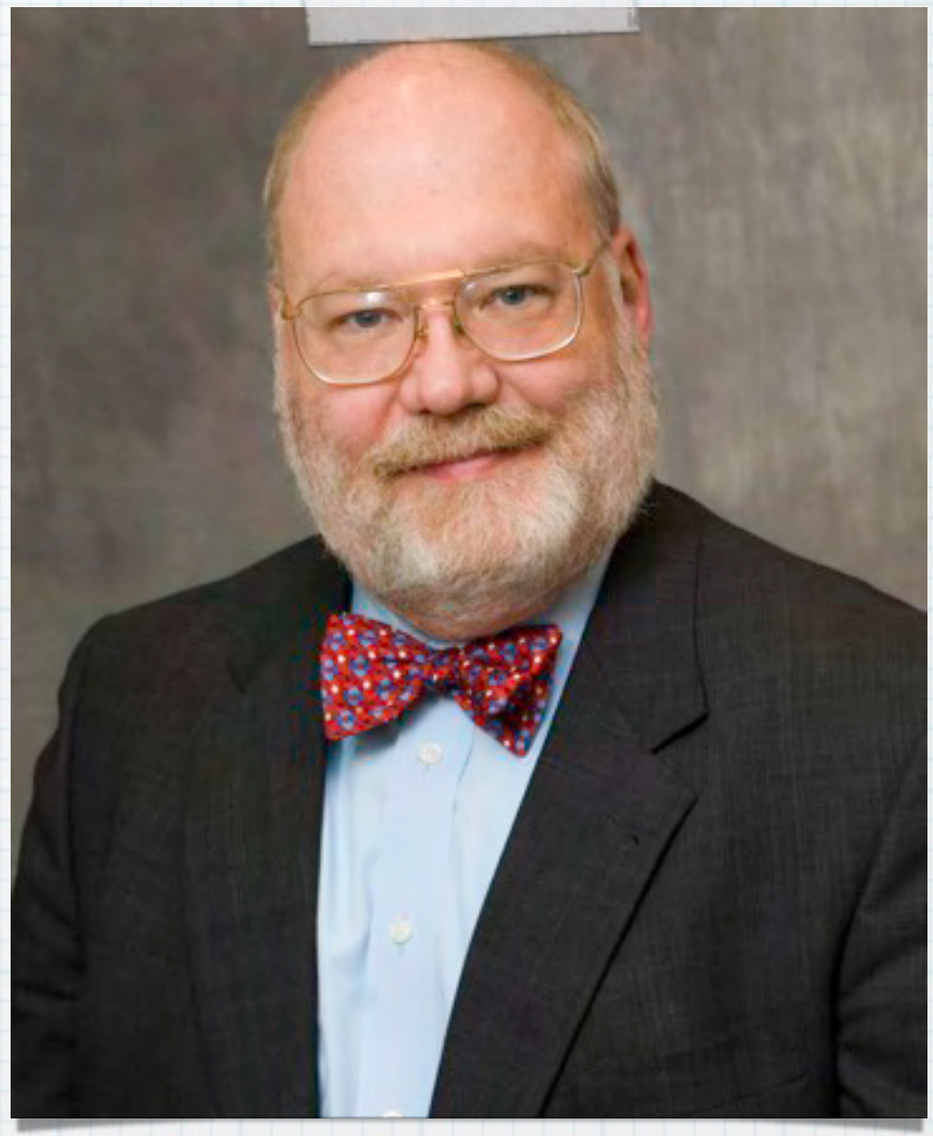
PROS :

- ✓ The Reason You Are Here
- ✓ Love To Take Classes
- ✓ Attracted To New Tech

Cons :

- ✓ Will Expect Your System To Act The Way <u>They</u> Want It To

"If you have responsibility for security but have no authority to set rules or punish violators, your own role in the organization is to take the blame when something big goes wrong."



Professor Gene Spafford
"Practical Unix and Internet Security"

"Be comforted that in the face of all aridity and disillusionment,
and
despite the changing fortunes of time,
There is always a big future in computer maintenance."

"Deteriorata" - National Lampoon, 1972