

# Skinning the Security Cat

A play in three acts, by MXN Corporation



***“Now, what WAS that password?”***

# *Act One—It's Not Your Fault*

---

## Scene One:

“I just don’t know how to handle all of these security issues on top of my regular job, and I don’t even have the budget to do it.” sobbed the IT Director.

“That’s OK,” smirked the consultant, taking off his jacket, “It’s not really your problem anyway!”

# *Effective Security is Holistic*



- which means that security is a process, not a collection of security products
- which means to you that security is bigger than IT
- which means that other people ought to get involved
- which means that IT is only the implementer of PART of the approved solution
- which means that they actually GIVE you the money to do your security job, if it's handled this way
- which means that you move from the patsy role to the participant and advisor role

***You can be the catalyst, but you ought not to be the responsible agency***



# *Philosophy Not Your Strong Point?*

---

## **Perhaps I can help!**

- *You are not in charge of emptying the trash,*
- *You are not in charge of vetting the janitors,*
- *You are not in charge of the shredding program,*
- *You are not in charge of Public Relations,*
- *You are not in charge of Payroll, Accounts Payable, Accounts Receivable, Student Accounts, Student Health, Admissions, Maintenance, Operations, Those Damn Professors, those irritating students, or really much of anything off the network.*
- *These are all important parts of the security milieu*

**Sorry, You're NOT the center of the security universe, but that's really a very good thing.**

*Act One, Scene Three:*



---

Arnold At The Dumpster

# Here are the Major Security Issues

---

**No, really!**

## **In general:**

- Data is stored in too many places
- There's a permissive data access climate
- There are no reasonable & enforceable rules OR
- The rules and reasons are not made plain
- There's a lack of business procedures for data access
- There's no parent involvement in security
- There's no student involvement in security—no peer pressure

***Little of this is in your purview. Notice that the words network, server, password, Internet, and PC don't even appear above!***

## *Parsing it down further.....*



---

What's the real data security issue?

- It's not access to the network or the servers or the Internet
- It's access—too much or too little—to the data
- The network, servers, databases, firewalls, etc. are the chorus

***Procedures*** and ***plans*** and ***programs*** need to precede ***products***.

If you're buying security products with your shriveled budgets without a top-down plan, the cart's before the horse.

*If the University's security officer reports to you, the IT Director, it's a bad thing. Security is mostly not an IT thing. And quarantining it In the IT shop will keep it from being effective.*

# *Act Two—Gotta Have a Plan*



---

## Scene One:


“How do I bring order out of the chaos and ferment of all of the options?” sniffled the IT Director, calming down a bit.

“Well,” said the consultant, still taking off his jacket (consultants are paid by the hour), “it helps to know what you need to do. And that means planning.”

(And smiles and rolls up his sleeves!)

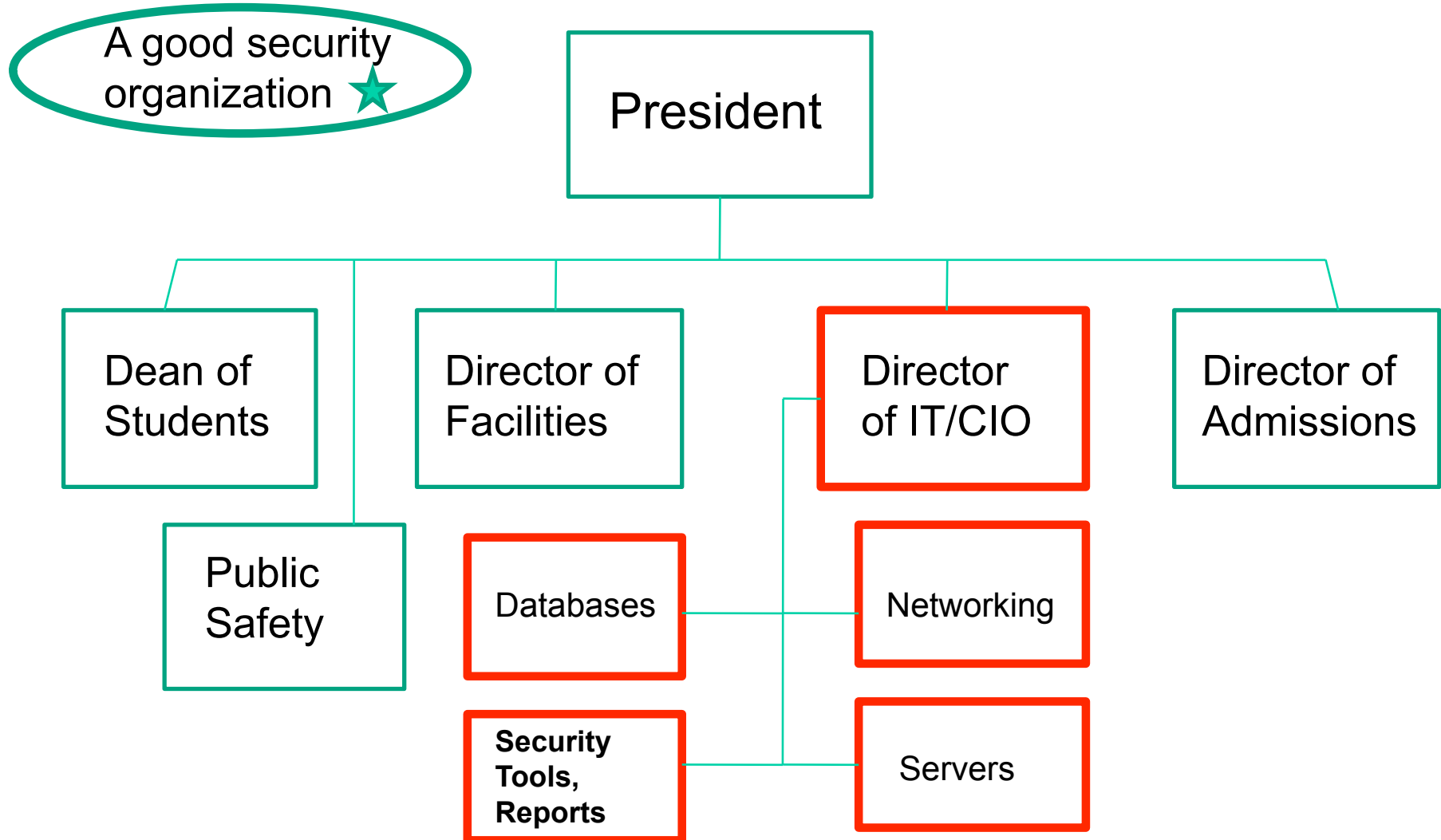
# *What to Do? What to Plan?*



- get upper management on board—security is not an IT problem
- define what security really is—you need goals and standards
- eliminate data to protect it (counterintuitive?—not!) 
- inaugurate a climate of shared responsibility
- promulgate clear policies, and clear consequences
- carefully draw the limits—generally limits are too tight
- create thoughtful, defensible policies
- firewall (sic) your network from outside issues and access control from the inside—the only truly IT function
- notifications, audits and follow-ups
- plan to block quickly, and respond quickly
- comply with all formal guidelines: FERPA, HIPAA, SOX, etc.

*(Notice—firewall and data mentioned only once)*

# Life as how it should be



# *Which Target is Easiest to Hit?* ~~man~~corp

---



*on eliminating data.....*

# *Some Security Facets*



---

Include these in the plan(s)

- network access control—from outside and inside
- facility access control
- output control (printing and copying)
- disposal rules
- acceptable use policies
- surveillance
- dorm responsibility and peer pressure (collective punishment)
- device registration
- notification of policies/media and frequency
- sanctions for violations

AAAAAAAAAAAA.....!



Bob's take on AAA.....is AAAAAAAAA

- assessment
- advisement
- ***authentication***
- ***access control***
- ***accounting***
- anomaly detection
- action!
- adjustment

And All need to be plAanned for.....

# *Touchy-feely stuff:*



---

When dealing with humans, IT folks:

- 90% of all folks are moral and responsible  
give them reasonable guidelines and periodic reinforcement  
give them the reasons why restrictions exist  
give them periodic reinforcement
- 90% of the remainder are troubled, but can be kept in line  
give them the punishment options  
remind them periodically  
identify them and watch them  
make examples of the violators when necessary
- The remainder are hell-spawn and should be killed

*Plan for controlling each category in the appropriate way!*

*Rehabilitation is important*

*Bob's Favorite Planning Quote* **m~~x~~n**corp

---

“The best thing about not planning is that failure comes as a complete surprise and is not preceded by a period of anxiety and depression.”

# *Act 3: Degeneration!*



---

## Scene One (several months later):

“Now that we’ve been at this planning game for a while, it’s time to put the plans into action,” said the IT Director, optimistically.

“I suppose that you’ll want to go out and talk with mere vendors,” said the consultant, huffily, as he put on his jacket and left the room.

# *If You Have to Talk Tactics;*



Yep, after planning we're into products

- effective anti-virus filters at the gateway and on critical resources
- anti-worm, anti-spyware and anti-malware filters
- device registration mechanism to link PC with people  
(remember accountability?)
- MAC address control
  - lockout
  - spoofing
  - piggybacking
- IPS at critical network junctions
- database control (print/copy/view)
- biometrics



## *Tactics, continued:*



- 
- flyers/posters
  - splash pages
  - inserts into catalogs
  - locked doors
  - briefing rules for recruiters and admissions
  - “sniffers”
  - cameras
  - reporting tools (data into information)
  - scanning and remediation tools—proactive instead of reactive

*A holistic (whole-istic) approach is the correct approach*

*As far as tools go, you already have more than you realize*

*Use tools carefully and judiciously—behavior shaping is best*

# *Implementation strategies*



- 
- start with one or two of the most critical areas and secure those
  - start!
  - trial programs before roll-out
  - enforce rules incrementally—disruption is NOT a goal
  - publicize the projects—student and worker education
  - evaluation and reorientation

Always think outside IT—how is it perceived?

I Give Up!

(You are all dismissed for Lunch)