Why Your IT Bytes

Frank J. Hackett

Big Thanks!

- Bsides Charlotte Organizers
  - Jon Molesa @rjmolesa
  - Bryan Tobey @_fmm
  - Damon Brinkley @damonbrinkley
  - Tom Moore @c0ncealed
  - Red Davies @noidd
  - Adam Byers @al14s
  - KC Yerrid @K0nsp1racy
  - Chris Teodorski @can0beans

- SELF for having us

Shout Outs

- High Hack Society
  - Awesome group of people
  - iPivot by pr1me and g11tch
    - http://www.highhacksociety.com/2013/06/02/ipivot-for-all-you-pivoting-needs/

Me

- Security Consultant
- Senior Systems Engineer
- Senior r00kie under j0e McCray
- SATF Member
  - http://www.satframework.org

Why Your IT Bytes

- We know IT cannot get the job done!
  - That is why we have jobs ☺
- What are some of the major differences?
  - Similarities?
- IT drives the organization
  - No email = no productivity
  - No shared files = no big data *gasp*

Why Your IT Bytes

- If we did not have IT professionals we would not have IT Sec & InfoSec professionals

- How boring would that be?

Give Thanks!

- Network Admins
- IT Engineers
- Devs of all kinds
- Senior System Engineers…

Major Differences - IT

- IT is the “yes man”
  - You’re a C-Level and want your tablet on the network?
    - No Problem Man!
  - Want simple access from home or abroad?
    - No Problem Man!

Major Differences - IT

- What's the big deal?
- It's an acceptable risk!
- We need Java!

IT Staff's Opinion About Security Folk

IT waiting for the audit to begin

http://securityreactions.tumblr.com/post/33361186596/it-waiting-for-the-audit-to-begin

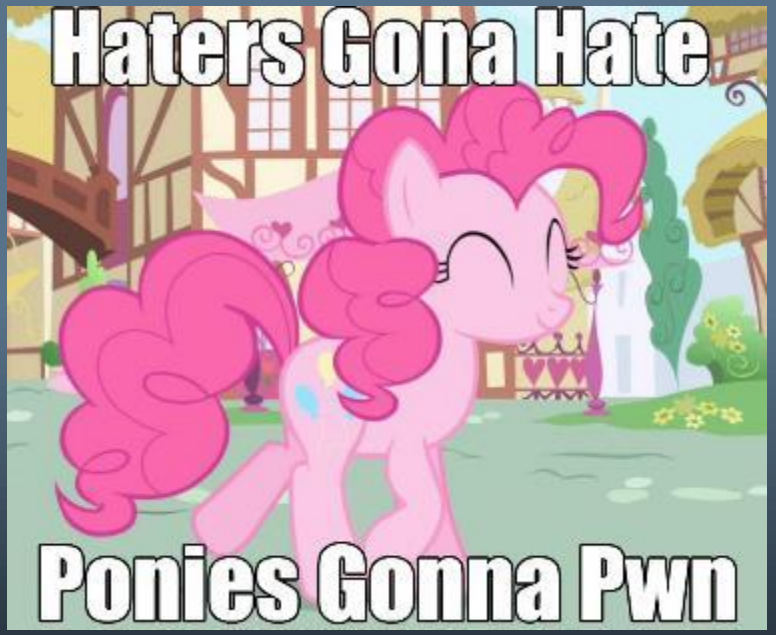
Major Differences - InfoSec

- Security thinks your baby is ugly
  - That's being nice…

- Security thinks your baby is REALLY ugly
  - Honest truth

Major Differences - InfoSec

- N00b
- zOMG why would you click that?!
- You really don't need Java!

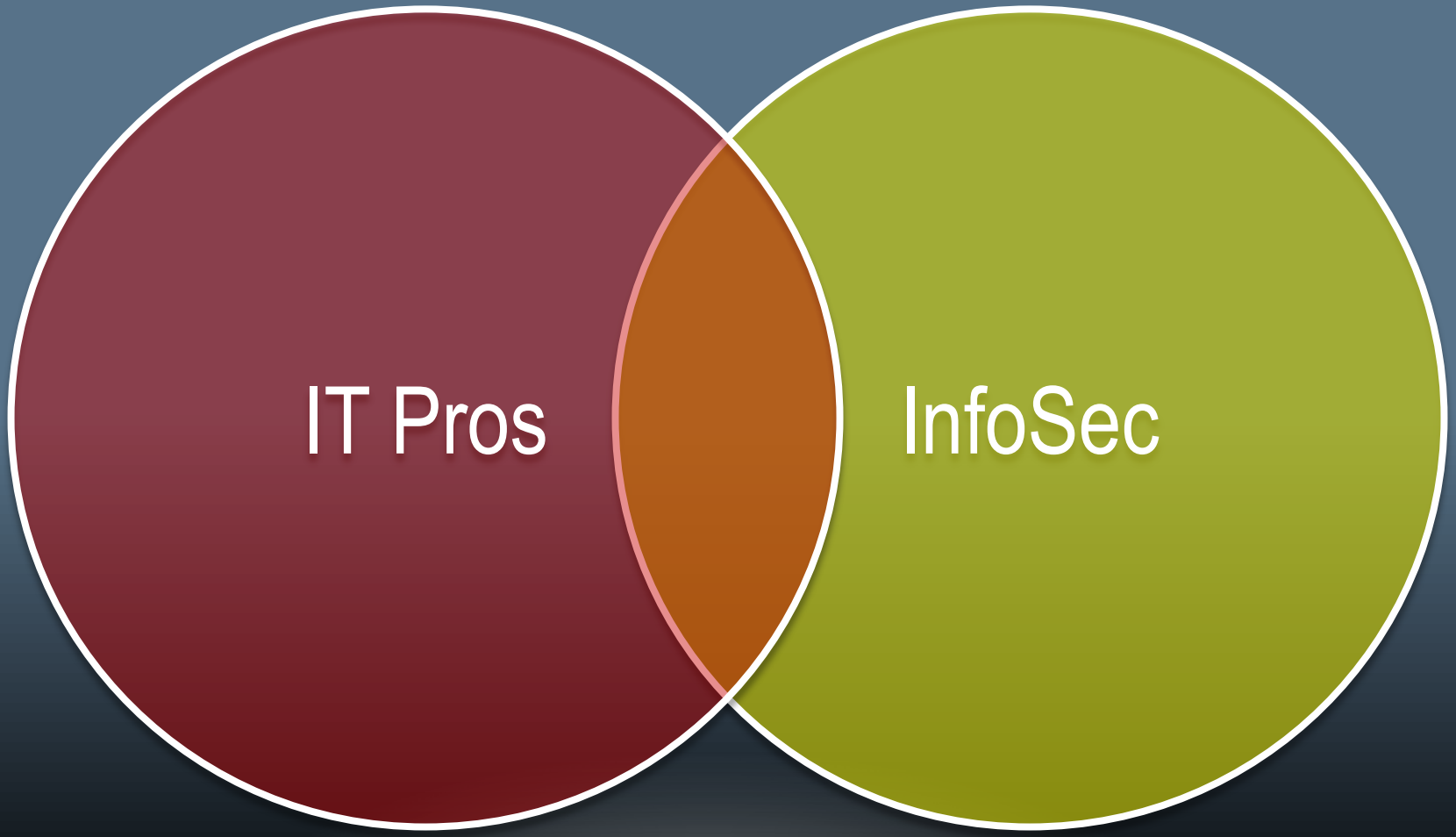


Security Looking at IT People

When they say their firewall cannot be breached

http://securityreactions.tumblr.com/post/29960560750/when-they-say-their-firewall-cannot-be-breached

Why Your IT Bytes



Common Ground

- *"Enhance the university experience for students, faculty and staff by facilitating a more secure computing environment."*
  - UFL IT Security Team Mission Statement
  - https://infosec.ufl.edu/aboutus/mission.shtml

- *"... providing a reliable, comprehensive information technology environment to enhance teaching, learning, research, services, and business operations. The division encourages effective, innovative, and ethical uses of technology while assuring efficient use of university resources."*
  - WCU IT Mission Statement
  - http://www.wcu.edu/academics/campus-academic-resources/it/aboutit/it-mission-statement.asp

Common Ground

We have the same goals!!!

Common Ground

Protect The Data, The Users, And The Organization

Common Ground

IT Doesn’t Know

- What can malware really do?
- Network security architecture
- Passwords!!!
- It’s OK to say no

IT Won't Save You

- Firewalls, GAV, IPS, any amount of blinky boxes will not keep hackers out
- Patching is not enough
- "Acceptable" and "Risk" should never be used in the same sentence

IT Can’t Save You

- Everyday new vulnerabilities are reported
  - How many aren’t officially reported???
- It’s hard for InfoSec to even keep up sometimes
- Too much to do

Educate

- Stop talking down to your IT department
- Work with them
- Expose IT to new ideas, solutions, etc.
- Show them how MS08-067 works and what it does!
  - It's a lot more then just a red tick on a Nessus report

Educate

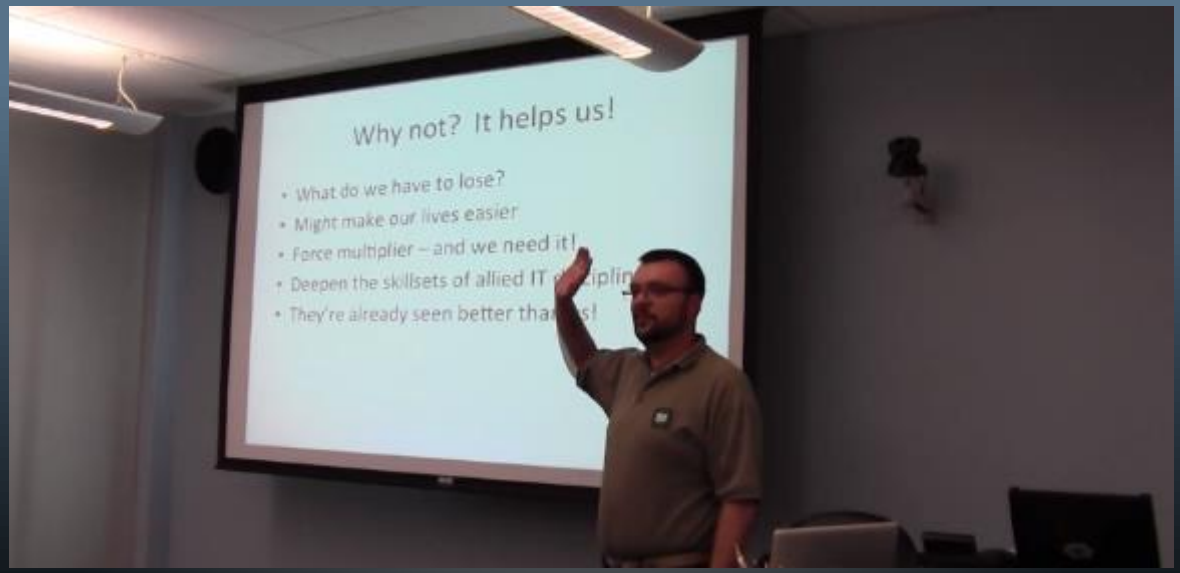
- Audit the IT department!
  - Explain the findings and what needs to be corrected
- Eliminate the idea that security costs tons of $$$
- Don’t “train” per say… demonstrate
  - They know how computers work and are smart people too!

Work Together

- Communication is key!!!
- Stop fighting with each other
- Can IT help Security to do their job?

Work Together

- Mick Douglas @bettersafetynet
  - “Help from the Help Desk” – AIDE 2013
  - http://www.irongeek.com/i.php?page=videos/aide2013/help-from-the-helpdesk-mick-douglas-bettersafetynet



Work Together

- Help secure IT from themselves!

- zOMG IT reuses passwords!
  - Why aren't all your routers, firewalls, switches, etc. 2fa??
    - Not hard to implement
    - Fast and reliable
      - Duo Security
      - Wikid Systems

Work Together

- IT specific policies
- How quickly can a user realistically be deactivated from IT?
- How quickly does a new tech gain access to your information?

Work Together

- IT is lazy
  - Break the cycle
- Remember → IT wants uptime
  - Patching = reboots
- Stay away from the guy/gal who “knows it all”

Work Together

- Positive correlation between the strength of the IT department and the strength of the Security department
  - Vice versa
- Each department should make the other better
  - Same team!!!
- This is very true for consultants as well

Work Together

- A pentest report is not enough
  - Work with your IT department!
  - Work with your customers!
- If you test a network, pwn everything, and offer no suggestions… what good have you done?

Relax A Little

- Let IT work for us
  - Smarter not harder
- You did the audit right?
  - Are better policies in place for IT now?
- Do you really want to add new Snort signatures for the rest of your life?

Relax A Little

- Shhh parts of our job aren't that hard – don't tell them
- Now that you've lead IT down the path of righteous they will help lead the users
- Remember what Mick said – "The help desk is already seen better then us!"

Relax A Little

- If IT is deploying better, stronger, and more secure infrastructure your job just got easier!
- If IT is going back and fixing weak infrastructure on their own give yourself a pat on the back
- Go write some new exploit code to keep them guessing ☺

Reality

- This is hard – people hate change
  - People really hate being told they're doing things wrong
- Start with your boss – get buy in
- Don't expect everything to change over night

Reality

- Tighten the screw one turn at a time – no nails and hammer

- When a change is introduced or a new policy is added, urge your coworkers to give it a week or two to try it
  - After this time it will be habit and the "old and good way" will be forgotten about

Reality

- Everyone is human. Even you - awesome security guru
- There will always be resistance to change
- More secure IT = more secure helpdesk = more secure users

Reality

- The trickle down effect is awesome!
- Also there's nothing wrong with improving the skills of a coworker
  - People like careers!

Remember

- Avoid the know it all
- IT can’t save you and they won’t save you
- They can make your job easier
- Don’t be the know it all

Hit Me Up

- @fjhackett
- http://www.hackettweb.com
- http://www.slideshare.net/fjhackett
- fjhackett@hackettweb.com