Computer Security for Businesses
Richard Ford, Ph.D., Florida Tech

Computer Security...

- Not just for Rocket Scientists!
- Not really even just for Computer Scientists...
- In fact, securing your electronic infrastructure is very simple
  - Smart “risk management” technique... like insurance
  - And like insurance, doesn’t require you to be an actuary
Why me?

- Why not?
- Research is computer security at Florida Tech
- Well-published
- 10 years of industry experience (IBM, Verio, Hiway Technologies...)

What if...

- All the electronic data in your business disappeared tomorrow?
- Okay, apart from getting the day off...
- Computers are a *critical* part of your business
  - Accounts payable
  - Customer contacts
  - Work product
So...

- Computer Security is just like any other business risk: you have to manage it
- That means looking at it from a Risk Management perspective
  - Balance the Cost of Prevention with the likely loss from the event
  - E.g. Spending $100 on antivirus software to stop a possible loss of $10,000 which is quite likely is a Good Deal™ but spending $10,000 dollars on a penetration test to stop an unlikely event is not.

Dr. Ford’s 10 Rules for Security

- These rules are tailored for small businesses
- But, from personal experience, I can tell you they work if you’re a Fortune 50 too!
Rule 0: Backup

- A backup is cheap and easy to do
- Can use tapes, a server solution or even burn DVDs
  - Don’t overwrite your backups!
  - Keep your backups offsite
  - Don’t *lose* your backups, it’s probably $$ in the bank to someone else
- Test your backups

Rule 1: Patch your machines

- Even my mother does this (honest!)
- In Windows XP, can be done automatically
- Increases reliability and security
  - Consider TCO and upgrade cost
- Prevents an attacker taking control via lots of different vectors
Rule 2: Use Antivirus Software

- Viruses and Trojans and Worms (oh my!)
- Very common problem in business
  - Can reduce a network to a bunch of colored wires in seconds
- Must **must** keep antivirus software up to date
- Make sure your vendor deals with Spyware too!

Rule 3: Use a Firewall

- Not using a firewall is the electronic equivalent of leaving the door unlocked
- Anyone can attack your machines
- My machine gets attacked every hour not every day!
- Not necessarily expensive
- Most businesses don’t need to let much in
### Rule 4: Be wary of Wireless

- Wireless “leaks” from your building
- Hackers “wardrive” looking for open networks to “play with”
- Make sure you set it up right if you’re going to use it
- Check periodically to make sure you don’t have a wireless network you didn’t know about!

### Rule 5: Watch your trash!

- Ah, the things we throw away
- Sometimes, it’s the equivalent of throwing our keys in the trash and assuming nobody is going to look for them
- Dumpster diving is very common… and shredders are really cheap
Rule 6: Use but don’t share...

- Passwords
- When you “let an employee go” you want to make sure their access is gone
- Bad idea to share administrative passwords with everyone

Rule 7: Understand your risk

- Don’t be paranoid, but don’t be careless either
- Know what the real threats are and engage employees to help you
- Remember, you are managing risk not removing it (or ignoring it...)
Rule 8: Know what you don’t know

- Sometimes you will have security needs which go beyond your expertise
- Know when that happens, and get help
- Don’t do silly things like open up your firewall because “Ned from Accounting needs to RPC in to his machine”

Rule 9: Don’t make the medicine worse than the disease

- Recognize that accidents happen, and people aren’t perfect
- Don’t make it like a prison!
Rule 10: Use least privilege

- Basically, most of your users don’t need complete control of their machines... so don’t give it to them
- Protects you from “whoops” moments

In Summary

- You CANNOT afford to ignore computer security
- But addressing it DOESN’T HAVE TO BE HARD
- Simple precautions work well
- When it gets difficult, call for help!
Questions?