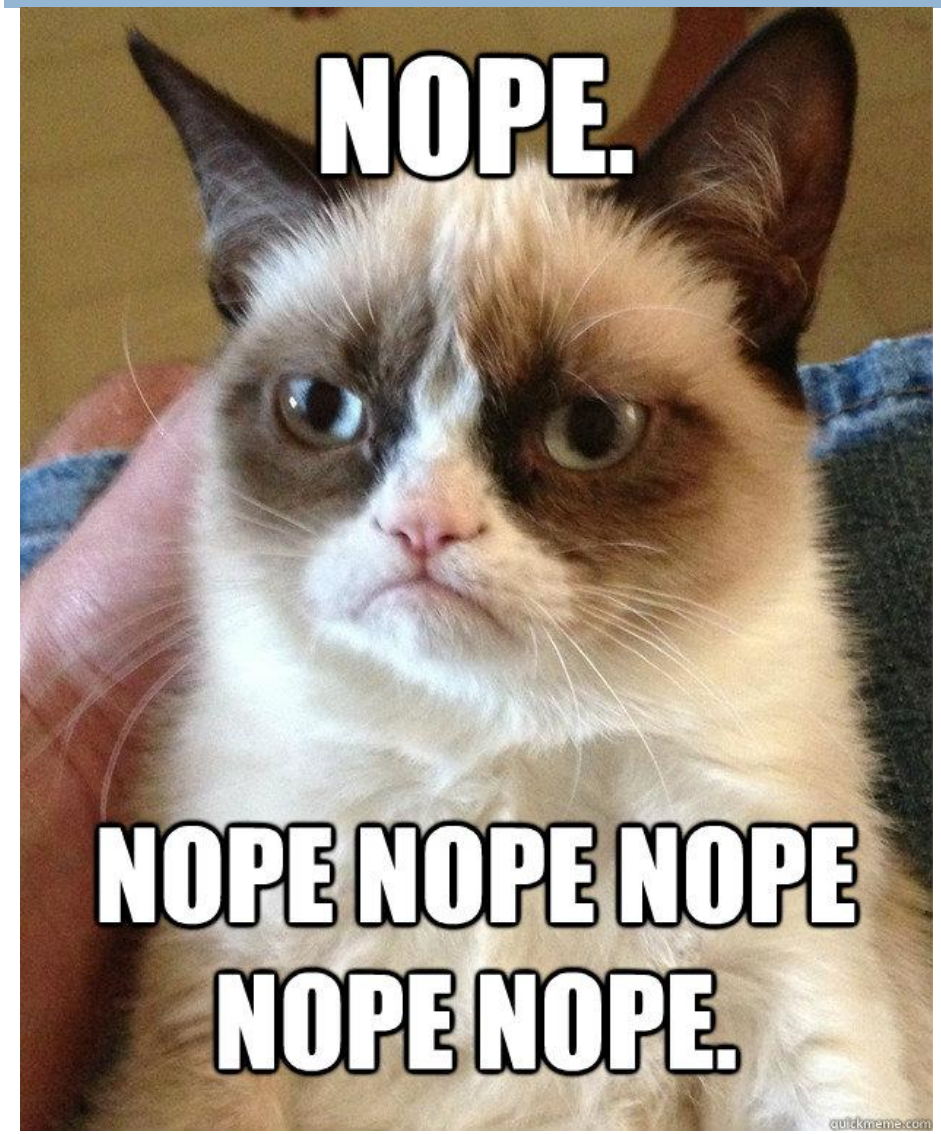
CYBER-SECURITY


NOPE.
NOPE NOPE NOPE
NOPE NOPE.
quickmeme.com


KEEP
CALM
AND
MAKE A
PLAN
KeepCalmAndPosters.com

IT Disaster Planning

1. Prevent
2. Plan
3. *Pray it never happens!*

IT Disaster Planning

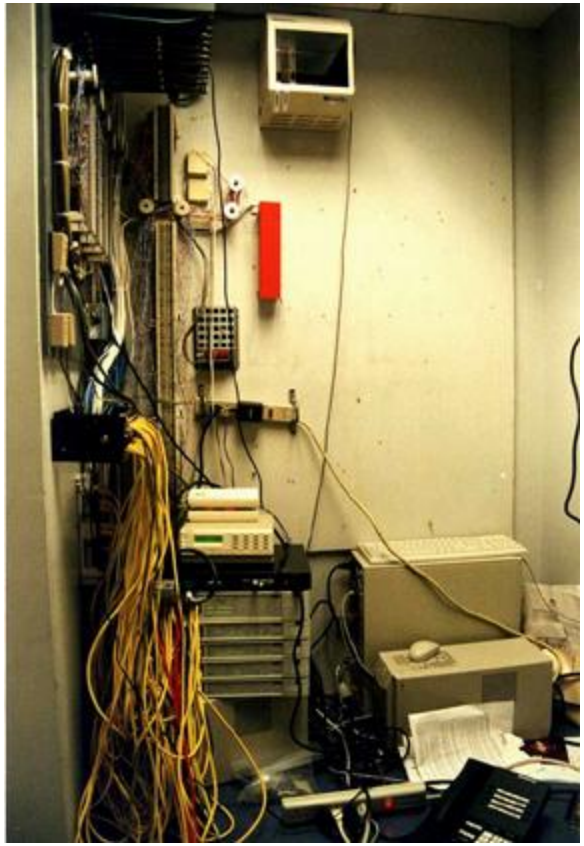
1. Prevent
2. Plan

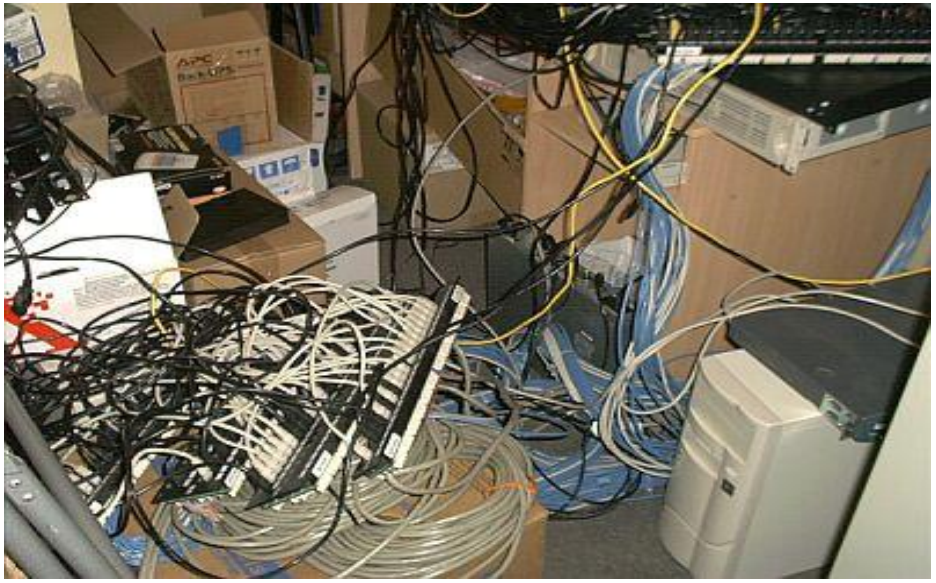
IT Disaster Prevention

- **Facility**
  - Clean
  - Air Conditioned
  - Wired Professionally
  - Battery Back-up
  - Limited Access

IT Disaster Prevention

- Location





IT Disaster Prevention

- Location

IT Disaster Prevention

- Equipment

IT Disaster Prevention

- Equipment

Laptop Issues

- **One** laptop is stolen every **53 seconds**
- **One** of every **10** laptops is stolen or lost over its life

Phone Issues

IT Disaster Prevention

- **Mobile Equipment**

  - Theft prevention
  - Backup
  - Data-delete solutions

  - Theft prevention
  - Backup
  - Anti-virus software

IT Disaster Prevention

- **Buy quality**
  - You do get what you pay for !
- **Be consistent**
  - Hardware
  - Software

Data Privacy

Data Privacy

- How well you protect sensitive information
- Reported breaches
  - 2005 – 40, 9.6 million records
  - 2008 – 932, 315 million records
  - 2011 – Sony Playstation – 77 million accounts
- Average breach costs $200 per record

What is *"sensitive information"* ?

How do protect *"sensitive information"* ?

Protecting Sensitive Data

- **Access controls**
  - Physical security
  - Passwords
  - Monitoring

What % of data breaches could be prevented with stronger passwords????

60%

What should you never do with passwords?

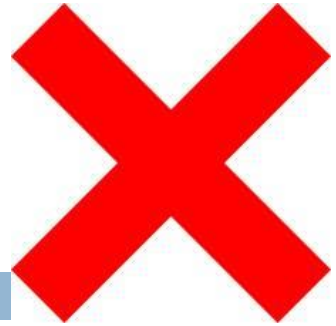
10 Password Don'ts

1. Use common dictionary words in any language – monkey, computer, password, buenosdias,
2. Spell words backwards – retupmoc, drowssap
3. Use sequential numbers - 123456 or 987654

10 Password Don'ts

4. Use personal information – name, nickname, child's name, pet's name, birth date, hobby, favorite sports team
5. Substitute similar numbers for alphabetic characters – p@ssw0rd, @nge11a
6. Add numbers to a common word – Tommy1, 2trouble

10 Password Don’ts



7. Use a string of identical characters – BBBBB, 767676
8. Use your log-in ID as your password
9. Write your password down
10. Share your password with anyone else

What should you never do with passwords?

5 Password Do's

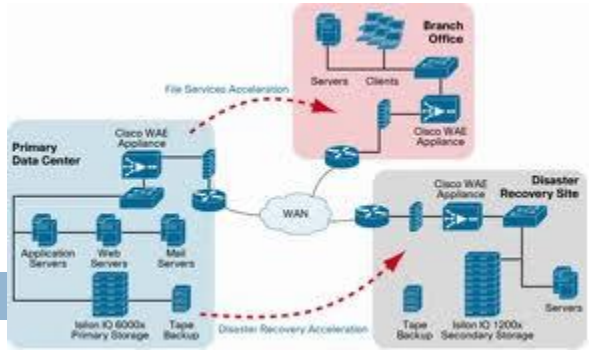
1. Do use a minimum of eight characters, but remember longer is better.
2. Do use a combination of alphabetic, numeric, and punctuation symbols
3. Do use a combination of lower case and capital letters
4. Do use different passwords for different internet log-ins.
5. Do change your passwords regularly

Network Security

- Risk that your network infects a client's with virus or is used by hacker to gain unauthorized access to information
  - Firewall
  - Virus Protection – computers & mobiles
  - Anti-spam software
  - VPN – remote access
  - Administrator rights & responsibilities
  - Restrict downloads & upgrades
  - Employee training

Data Redundancy

Data Redundancy



- **Files should be on "File Server"**
- **Backups**
  - Automatic
  - External hard-drive better than CD/Tape
  - Offsite
  - Don't forget to backup software applications !
- **Co-location/managed services**
  - Outsource e-mail

Outsourced IT Services

- ☐ Get a SOC 2 Type 2 Report
- ☐ Ask if they have dedicated IT Security personnel
- ☐ Ask to see a copy of their Disaster Recovery Plan

IT Disaster Planning

1. Prevent
2. **Plan**

Do you have an IT Disaster Recovery Plan?

How many of you have tested your IT Disaster Recovery Plan?

28% of companies test their plan

per Symantec 2011 survey

IT Disaster Recovery Plan Questions

- What is an inconvenience vs disaster?
  - Lost data/application disabled/network compromised/environmental event
- Recovery time objective
- What systems are critical?
- Who must be operational?
- Alternate locations/access

October 27, 2008

Creating an IT Disaster Recovery Plan

- Assess risks
- Test:
  - Power back-ups
  - Ability to use system remotely
  - Data restoration
- Communicate plan
- Update regularly

October 27, 2008

Creating an IT Breach Plan

- Identify, locate, and map digital assets
  - Intellectual Property
  - Confidential data
  - Proprietary software
- Identify risks and potential breaches
- Develop response plans that address:
  - Mitigation and correction for each threat
  - Members of response team

Creating an IT Breach Plan

- Develop Communication Plan
  - Affected parties
  - Regulatory agencies
  - Which employees can talk
  - What employees can say
- Communicate plan to employees
- Update regularly