# Segurança na Internet2: Problemas e soluções atuais

Liane Tarouco

UFRGS

Reunião GTS - Novembro/2008

# Reunião da Internet 2

Fall 2008
Internet2 Member Meeting

New Orleans, Louisiana

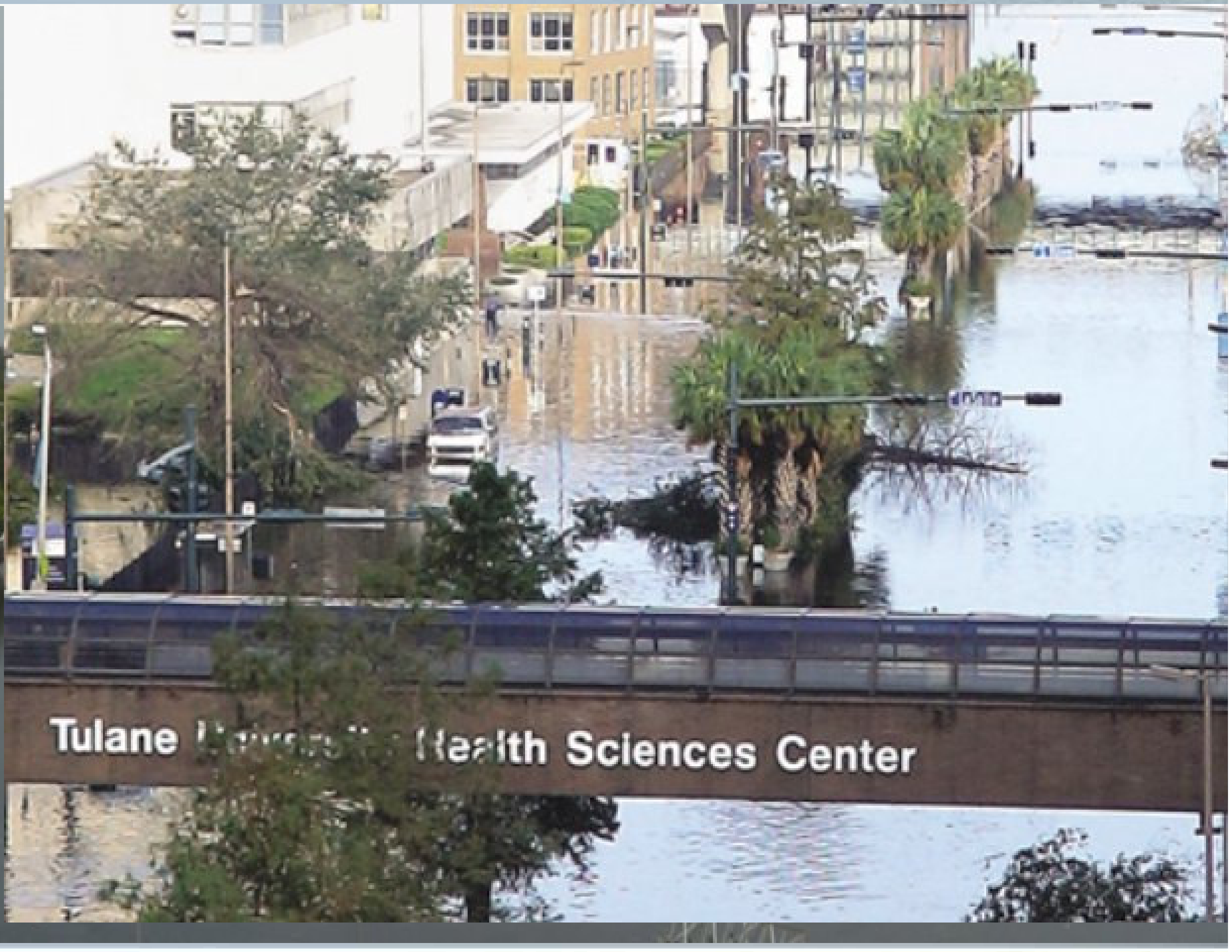
October 13-16, 2008

# Disaster Planning & Recovery

Keeping Your Head Above Water:
The Tulane Katrina Experience - Scott Kowen – Univ Tulane
Katrina experience raised awareness of the importance of planning for disasters

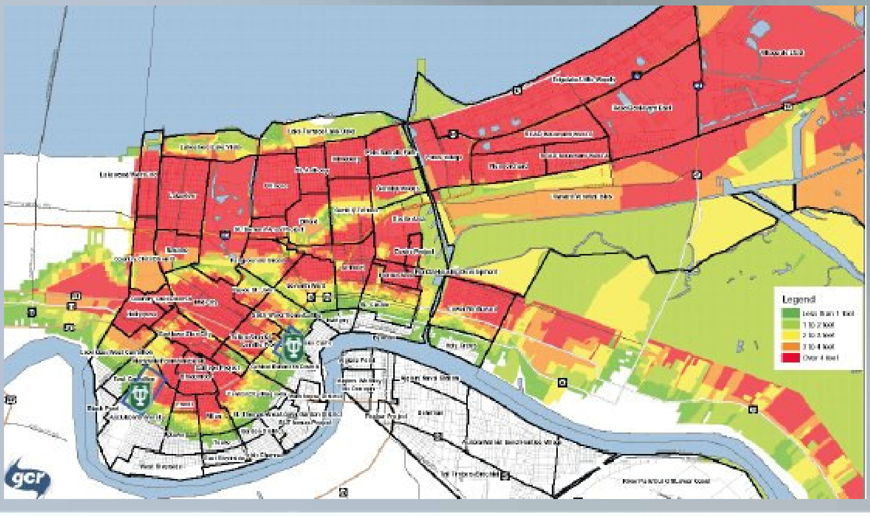
# University of Tulane

- Day after Katrina



# Univ Tulane after Katrina

- Flooded 70% of the main campus and the entire health sciences center campus
- Resulted in 13,000 students and 8,000 employees dispersed for five months
- New Orleans - August 31, 2005, 80% of New Orleans was flooded, > 4 metros



# Salsa Disaster Recovery

- SALSA - Security At Line Speed: working group at Internet2
- Wg SALSA – DR : Disaster management and disaster recovery
- Very quickly, emergency notification by cell phone and email, as well as web presence during an emergency
- Enabling Continuous Data Protection (CDP), the New Dimension in Remote Storage Management for Business Continuity and Disaster Recovery
  - Secondary Data Center
  - Federations

# Salsa Disaster Recovering

- Best Practices
  - Emergency Email hosting
  - Emergency virtual hosting
  - Cooperative backup services
  - Prioritizing business systems for external hosting
  - Cooperative NOC monitoring
- Cooperative agreements between institutions

# Security for advanced networks

- Overview of EDUCAUSE / Internet2 Effective IT Security Practices Guide - John Bruggeman
- Identity Assurance in the Real World
- Concerns in the Use of Endpoint Agent Security Tools - Dikran Kassabian
- Landscape of IT Security
- DNSSEC at Louisiana State University
- Loss of Network Control Incidents - Joe St Sauver
- ARP Poison Routing (Spoofing and Impersonation) - David A. Greenberg

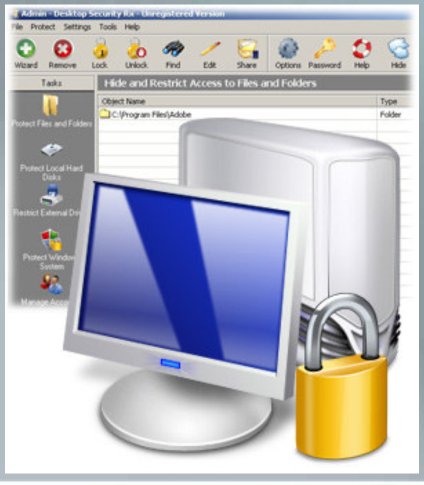
http://events.internet2.edu/2008/fall-mm/

# EDUCAUSE / Internet2 Security Task Force Effective Practices

- Internet2 and EDUCAUSE formed the Computer and Network Security Task Force – Jul/2000
  - The task force works to improve cybersecurity across the higher education sector and actively promotes effective practices and solutions for the protection of information assets and critical infrastructures.
  - Sub-groups:
    - Awareness and Training
    - Effective Practices and Solutions
    - Policy and Legal Issues
    - Risk Assessment
    - Internet2 Security Initiative called SALSA (Security at Line Speed ) http://security.internet2.edu/salsa
    - REN-ISAC (Research and Education Networking – Information Sharing and Analysis Center (www.ren-isac.net)

# EDUCAUSE / Internet2 Security Task Force Effective Practices

- The EP Guide
  - http://wiki.internet2.edu/confluence/display/secguide
  - Wiki linked from Internet2 and EDUCAUSE sites
    - http://www.educause.edu/security
    - http://security.internet2.edu
  - The guide has several components
    - IT Security Guide
    - Effective practices
    - Toolkits
    - Other resources



# EDUCAUSE / Internet2 Security Task Force Effective Practices

- Current List of Effective Practices
  - Application Security for Database Administrators
  - Application Security for Developers and Quality Assurance Personnel
  - Application Security for Management, Project Managers, and Architects
  - Collaborative Information Security Project - Vulnerability Assessments
  - Conducting a Preliminary Risk Analysis and Creating an IT Security Group and Policy
  - Developing a Certification Authority for PKI at Virginia Tech

# EDUCAUSE / Internet2 Security Task Force Effective Practices

- Current List of EP’s cont.
  - Edge Access Control Lists at Cornell University
  - Firewall Strategy at Brown University
  - Five-Year Rotating Audit Focus Based on Risk Assessment at Georgia Tech
  - Georgia State University's IT Procurement Review Process--Practical Approach to Assessing Risks of IT Projects
  - Homegrown Wireless LAN Security
  - Implementing Information Security Governance Using ISO27000 at Georgia State University

# EDUCAUSE / Internet2 Security Task Force Effective Practices

- Incident Response at University of Madison-Wisconsin
- Intrusion Detection at University of Notre Dame
- Lessons Learned from RIT's First Security Posture Assessment
- Monitoring and Network Forensics at the University of Chicago
- Network Registration System Scanner
- Purdue AirLink (PAL)
- Purdue Firewall Appliance
- Responding to Large Scale Incidents at UFL

# EDUCAUSE / Internet2 Security Task Force Effective Practices

- Responding to Major Incidents at Indiana University
- Security Log Analysis for Windows NT/2000/XP/2003
- Self-Service/Automated Security Vulnerability Assessment Program
- The Vulnerability Scanning Cluster
- Use of LANDesk for Patch and Configuration Management
- Using NAT for Perimeter Protection
- Whole Disk Encryption Evaluation and Deployment at Baylor University

# EDUCAUSE / Internet2 Effective IT Security Practices Guide

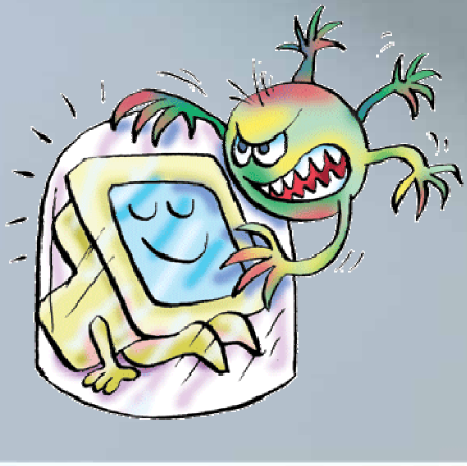
- Computer and Network Security Task Force- http://www.educause.edu/security/16030
- Effective IT Security Practices and Solutions Guide: Balancing the Need for Security and Open, Collaborative Networking
  - Colleges and universities
  - Reduced cost

# Five Elements for a Successful Security Website

- IT security websites that are informative and helpful to their users
- List of common features and effective practices that can serve as an outline for a college or university developing or updating their campus IT security website.
  - Anti-virus
  - Information
  - Engaging Design to Attract and Educate Viewers
  - A Place to Ask Questions and Report Incidents

# Anti-virus Software and Scanning Options

- Majority of security websites offer students and other university users free anti-virus software.
- Most also provide scanning services, so students may detect viruses, spyware, or other problems with their personal computers.



# News Updates and Alerts

- Some of the better sites feature up-to-date news articles, as well as virus, spyware, and phishing alerts.
  - e-mail list option for those who want to receive security alerts in their inboxes as incidents occur.
- With new challenges to information security arising constantly, timely information is critical.
- Providing the latest on potential threats to the campus is an important element for maintaining security

# Information

- Information by topic, Q&A, and recommended outside
- links are important for
- educating users about
- security issues.

- Relevant, timely information on hot topics, including viruses, identity theft, and social networking safety.

- Helpful outside links that help students further learn about security matters.

# Engaging Design to Attract and Educate Viewers

- While many sites provide thorough, reliable information, not all of them present it well.
  - Format, attractiveness, and accessibility matter. Content alone does not guarantee success.
  - Excellent sites feature topics, graphics, and headlines that grab your attention.
  - They encourage the viewer to learn more about information security by presenting subject matter in an interesting or creative way.
    - quizzes to test users on how much they know about security.
    - "Top Ten Security Tips" or Penn State's parody of Facebook, which provides safety information for social networking sites.
  - They are carefully designed so that searching for topics would be rather intuitive for the viewer.

# A Place to Ask Questions and Report Incidents

- While good sites may provide a plethora of information and seem to cover all bases, even the best cannot foresee all questions.
- 
- A reliable help desk and easy access to contact information is very important.

- The most successful sites will prominently display e-mail and phone information, so that users may ask questions and report incidents.

# Recommended Practices

- Create an IT security website that provides basic security information for all users (faculty, students, and staff).
- Use a common alias (e.g., http://www.university.edu/security or http://security.university.edu).
- Prominently display contact information (e-mail and/or phone number).
- Include RSS feeds for for security-related news, updates, and alerts
- Institution's main IT page should provide a highly visible link to their security page.

# Concerns in the Use of Endpoint Agent Security Tools

- Some security tools require users to install an “agent,” a small software component that runs on the users endpoint.
  - Some asset management tools
  - Some tools that look for personally identifiable information (PII)
  - Some virus protection tools
  - Some network access control tools

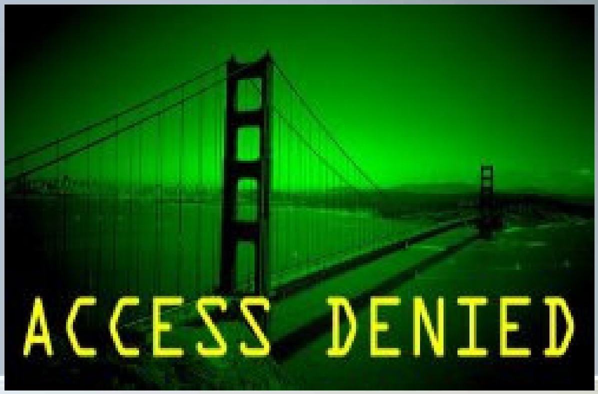
# Shifting Landscape of IT Security

- Major paradigm shifts
- A fundamental shift in motivation of the attacker community, from fiercely independent vandals to organized criminals herding large groups of compromised systems to engage in illicit money-making activities

- At the same time vendors have shifted their strategy, and most operating system, application, and database vendors now embrace the "secure-by-default" philosophy, leading to a sharp decline in the success of network-based attacks and automated worms that rely on such attacks

# Loss of Network Control Incidents

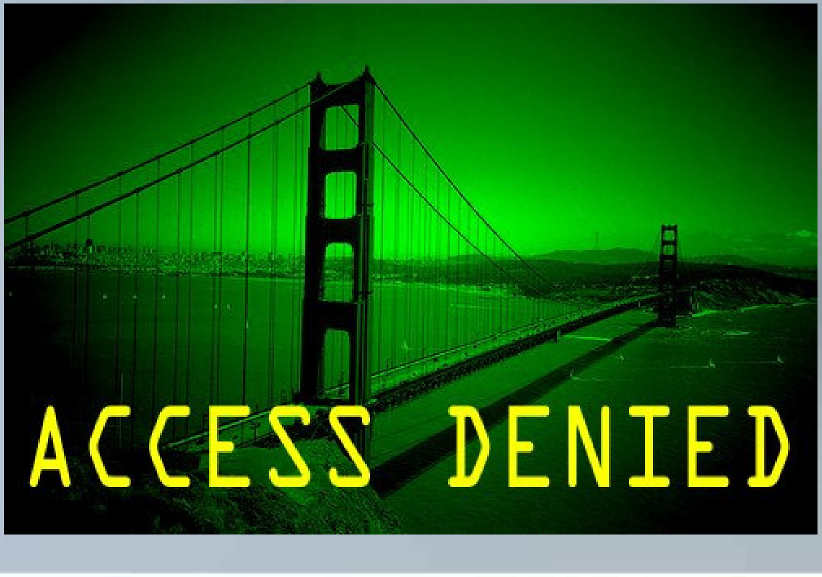
- A major western city recently found itself "locked out" from its own network for a multi-day period, allegedly as a result of actions undertaken by one of its own staff.
- In discussions of this incident on the Internet2 Salsa-DR (Disaster Recovery) working group, many important implications emerged.



# S.F. officials locked out of computer network

- A disgruntled city computer engineer has virtually commandeered San Francisco's new multimillion-dollar computer network, altering it to deny access to top administrators even as he sits in jail on $5 million bail.

14/07/2008



# Disaster analysis implications

Implications → importance of having:

- **(a) established procedures for password recovery/reset in the event that an administrator forgets, loses, or is otherwise unable to supply a privileged password when required;**
- **(b) offline backups (and any passwords which may be needed to access those backups, e.g., if they've been encrypted);**
- **(c) a well-documented and up-to-date written system configuration;**
- **(d) procedures for handling human resource issues which may arise in conjunction with individuals working in sensitive positions;**
- **(e) the value of periodic security audits; and**
- **(f) the risks of running thinly staffed in key technical IT areas, among other things.**

# San Francisco network takeover

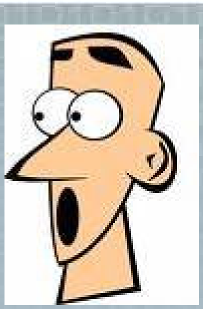
- Terry Childs, a 43-year-old computer network administrator has been charged with four counts of computer tampering and is scheduled to be arraigned today.
- Prosecutors say Childs, who works in the Department of Technology at a base salary of just over $126,000, tampered with the city's new FiberWAN (Wide Area Network), where records such as officials' e-mails, city payroll files, confidential law enforcement documents and jail inmates' bookings are stored.
- Childs created a password that granted him exclusive access to the system, authorities said. He initially gave pass codes to police, but they didn't work. When pressed, Childs refused to divulge the real code even when threatened with arrest.
- Source: www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2008/07/14/BAOS11P1M5.DT

# This Incident Could Have Been a Lot Worse

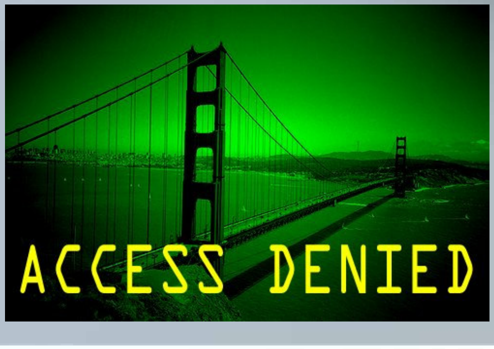
- As bad as it was, it could have been a lot worse.
  - -- The network didn't go down; it continued to run during the incident, including continuing to deliver mission critical functionality for services such as public safety
  - -- The city's network's hardware and software wasn't damaged -- Personally identifiable data wasn't publicly disclosed, nor was data modified without authorization
  - -- Staff members weren't harmed, etc.
- **Cost**: city has already paid $182,000 to Cisco contractors and $15,000 in overtime related to the incident, and has set aside an additional $800,000 to cover further future costs associated with the incident.

# San Francisco network incident

- So how was this even technically possible?



- How could one person allegedly obtain total control over an entire city's backbone network?



# Taking control

- When it comes to **taking** control of a major network, it helps if the owner begins by **giving** control of it to you.
- In this case, the alleged perpetrator was the person in charge of the city's network, and as such he had:
  - total access
  - an intimate knowledge of the network (after all, he'd built it)
  - a high level of technical expertise
  - he apparently had limited managerial oversight.

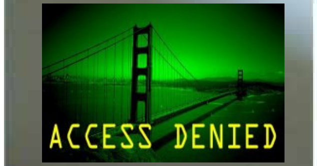
# Gotcha #1: One (and Only One) Administrator With Full Access

- **"Surely more than one person had privileged access to the City of San Francisco's routers and other network devices?"**
- It only took a minute for me to recognize that there was always the unsettling possibility that someone with privileged access might have changed the enable password to some new value known only to himself, but in reading the court filings it was clear that no, Childs was, and was known by the city to be, the only one with full administrative access to the city's network.
- That should have set off alarm bells -- at least it sure did for me.

# The Insider Threat

- “[…] Terry Childs, 43, was arrested July 13 at his suburban home, where police found $10,000 in cash, diagrams of the city-county computer network, a co-worker's access card, a loaded 9mm magazine and several loose .45-caliber rounds.
- Under the user name Maggot617, he hijacked the system and refused to turn over passwords for the network, which superiors belatedly discovered only he controlled. […]
- “I don't want to make it sound hopeless," but "when I go around and give talks, it seems like people don't really understand their risk of being the victim of insider sabotage,“ said Dawn Cappelli, a specialist in insider threats with CERT-CO

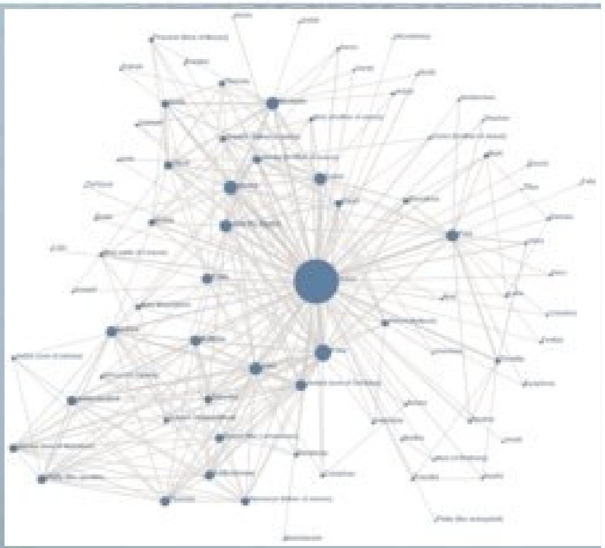
# Physical access is enough?



- The city obviously still had physical access to all their network devices. All geeks “know” (or should know) that if you have physical access to a device you should be able to use a serial console (or push the magic "reset button," etc.) to reset the device and regain control over that device, right?
- That simple reality ("if I can touch it, I can 0wn it") is one reason why smart IT security folks tend to be so "paranoid" about physical security (as well as network and system security)…
- The reset process usually isn't hard.

# Password recovery on many Devices

- In a large network, there might potentially be *many* devices with passwords needing to be reset.
- For example, in the city of San Francisco’s case, there were reportedly some 1,100 discrete routers/switches/modems/

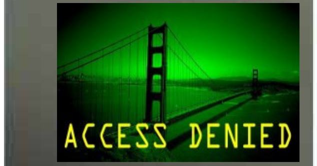


- Normally, for a network of that size, authentication/authorization/ access control are scaleably handled by using centralized authentication technologies (such as radius).

# Recovering passwords

- But if local passwords were used, password recovery may require visiting each and every one of those devices to do the password reset process and/or to load a known good config, a potentially long and tedious process -- particularly if devices are located in remote locations, or the networks in question have strict and strictly limited maintenance windows.

# Add Potential Gotcha #2: Volatile Configuration



- Note that at least the Cisco lost password recovery procedure include a critical step, “reboot the router.”
- If a router’s configuration were to be stored ONLY in RAM, and NOT committed to flash memory or other persistent storage, rebooting the router (or any other event which resulted in a loss of power to the router) would trigger a complete loss of the router’s configuration and a network outage.
- At the risk of stating the obvious, your network devices‘ configuration MUST always be saved to non-volatile storage to insure that systems CAN successfully survive a power outage or reboot.

# Worries About Scheduled Minor Power Outages

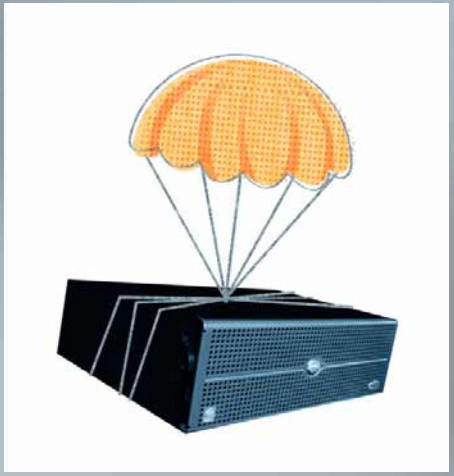
- Unusual levels of employee concern about short duration scheduled downtime may be a potential warning flag. Routers and other network devices should be able to easily survive a graceful shutdown and restart cycle.
- However, not having performed a forensic review of the City of San Francisco's network devices, we don't know for sure if the router configurations were committed to persistent storage or just lived in volatile memory. We do know, however, that the defendant was reportedly worried about an imminent scheduled power outage, potentially a sign that there may have been at least some network devices which wouldn't be coming back up after a reboot.

# Add Gotcha #3: no service password-recovery

- If the router has “no service password-recovery” enabled, you can still reset the router… but only to a default factory configuration.
- You’d then need to be prepared to reload the configuration from a backup copy of the configuration files to restore the router to service.

# Add Gotcha #4: No Config File Backups

- This one's the *real* killer.
- If the router’s as-configured state were to be lost (for whatever reason), having a usable backup copy of the device’s configuration is critical to quickly bringing that device back up.



# [Some] Configuration File Recommendations

- 1. Configuration files should be periodically archived in digital and hardcopy forms (retain  earlier versions)
- 2. One or more copies of the configuration files should not be under the control of the individuals who are responsible for running the network.
- 3. Changes to network device configurations should be peer reviewed before actually being made
- 4. Configuration files should be reviewed (or at least be made available for review) as part of an annual external IT audit.
- 5. Changes should be made in a transparent fashion, with appropriate tools used to document and disseminate copies of config file diffs to relevant technical and security staffs.

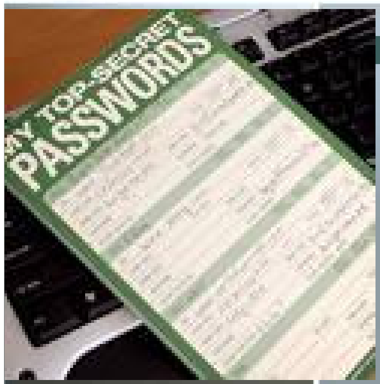
# One Configuration File Mgmt Tool: RANCID

- **RANCID = Really Awesome New Cisco confIg Differ** - www.shrubbery.net/rancid/
  - Used by AOL, Global Crossing etc…
- RANCID monitors a router's configuration, including software and hardware (cards, serial numbers, etc) and uses CVS (Concurrent Version System) or Subversion to maintain history of changes.
  - login to each device in the router table
  - run various commands to get the information that will be saved,
  - cook the output; re-format, remove oscillating or incrementing data,
  - email any differences […] from the previous collection to a mail list,
  - commit those changes to the revision control system

# Document Your Network Architecture/Design

- Beyond just watching device configuration files, you should also insure that your network’s overall architecture/design has been fully documented.
- Sometimes there is a tendency to build or modify a network first, waiting to document the network until things “slow down a little.”
    - Of course, as we all know, things never really slow down, and hence many networks get built but never get documented the way they should be.
    - Auditors should flag this when they notice it.

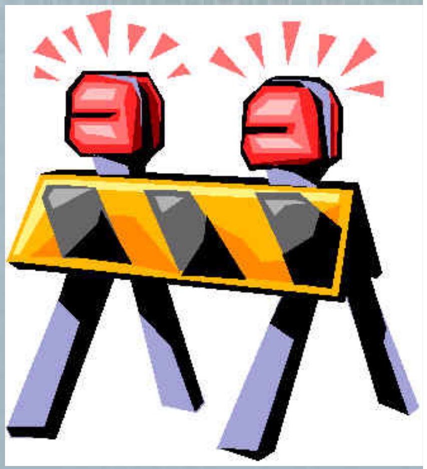
# Passwords



- On July 21st, during a 15 minute meeting with the mayor of San Francisco, the defendant disclosed three usernames and one password. Those credentials allowed the city to regain access to its network -- but only from "one location," a connection in “room 125 of the Hall of Justice.”
- “Surprisingly, the police department’s IT administrator was not aware of this access point installed by the Defendant.”
- Also on July 21st, “the Department of Park and Rec […] located another access point that the Defendant never revealed.”
- Childs also allegedly had dialup and DSL access paths into the city’s network.

# Alternative access points

- For the city, discovery of these alternative access points raised the uncomfortable possibility that **they might not be technically able to lock Childs out of their network**



- Childs might have additional still-undiscovered access points he controlled, access points which might be difficult for the city to identify/eliminate.

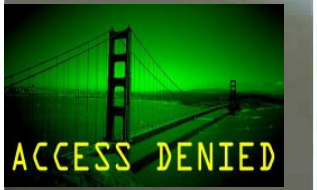
# Extra access points

- Were the defendant’s various extra access points “undisclosed and unapproved surreptitious backdoors” meant to keep the city from being able to block he defendant’s access to the city’s network, or were they routine, reasonable and prudent “out of band emergency access” pathways meant to insure that Childs, as network manager, would always have access to work on the network if it went down in an emergency?

# Discovering Unauthorized Modems (and Wireless!)

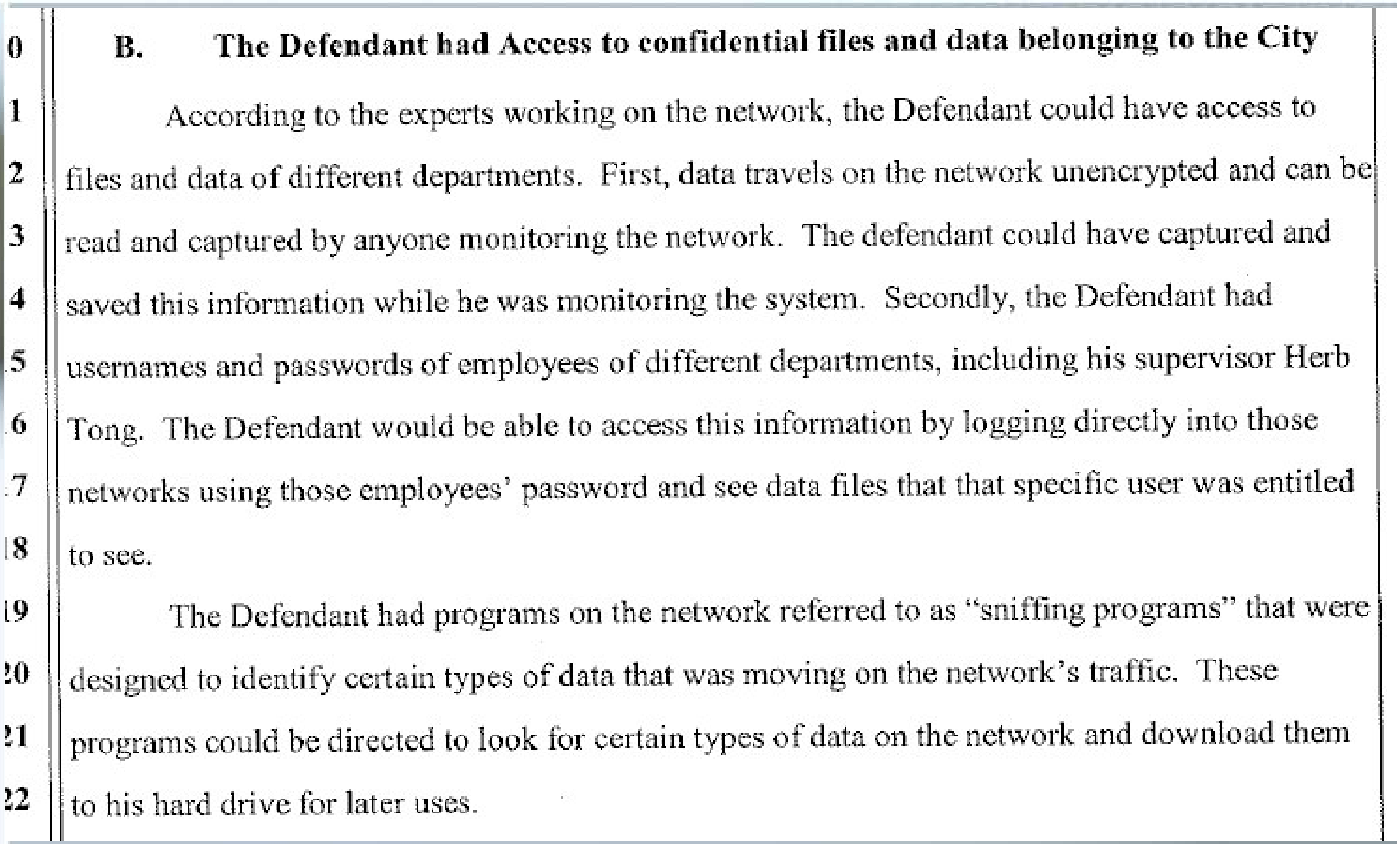
- When it comes to finding unauthorized modems attached to a network, there are several strategies that one could try, including:
  - “war dialing” one’s own network (however be aware that modems may not always be up/answering, they may be set to use a timer and only be up for a short/oddly scheduled period)
  - auditing telecom payments to look for payment discrepancies:
- But these days, you also need to recognize that remote access might just as readily take place via a rogue WiFi wireless access point, a commercial WiMax connection, or a cellular modem paid for using non-institutional funds.

# Other City of San Francisco Access Related Concerns



- There are also statements in the filing that point out that the network devices were only accessible from certain places within the network.
- They claim this as another example of malfeasance on the part of Childs, saying "Thus, even possessing the passwords were not enough to regain control of the network, but one had to know where to go to communicate with the network's core devices."

# Data unencrypted



**B. The Defendant had Access to confidential files and data belonging to the City**

According to the experts working on the network, the Defendant could have access to files and data of different departments. First, data travels on the network unencrypted and can be read and captured by anyone monitoring the network. The defendant could have captured and saved this information while he was monitoring the system. Secondly, the Defendant had usernames and passwords of employees of different departments, including his supervisor Herb Tong. The Defendant would be able to access this information by logging directly into those networks using those employees' password and see data files that that specific user was entitled to see.

The Defendant had programs on the network referred to as "sniffing programs" that were designed to identify certain types of data that was moving on the network's traffic. These programs could be directed to look for certain types of data on the network and download them to his hard drive for later uses.

# Terry's List of Employee Usernames and Passwords

- The extract from the prosecutor's motion in opposition to a reduction in bail also refers to a list of "usernames and passwords of employees."
- From the context (e.g., a discussion of monitoring/sniffing network traffic), one is lead to believe that these usernames and passwords may be ones which the defendant captured from the network.

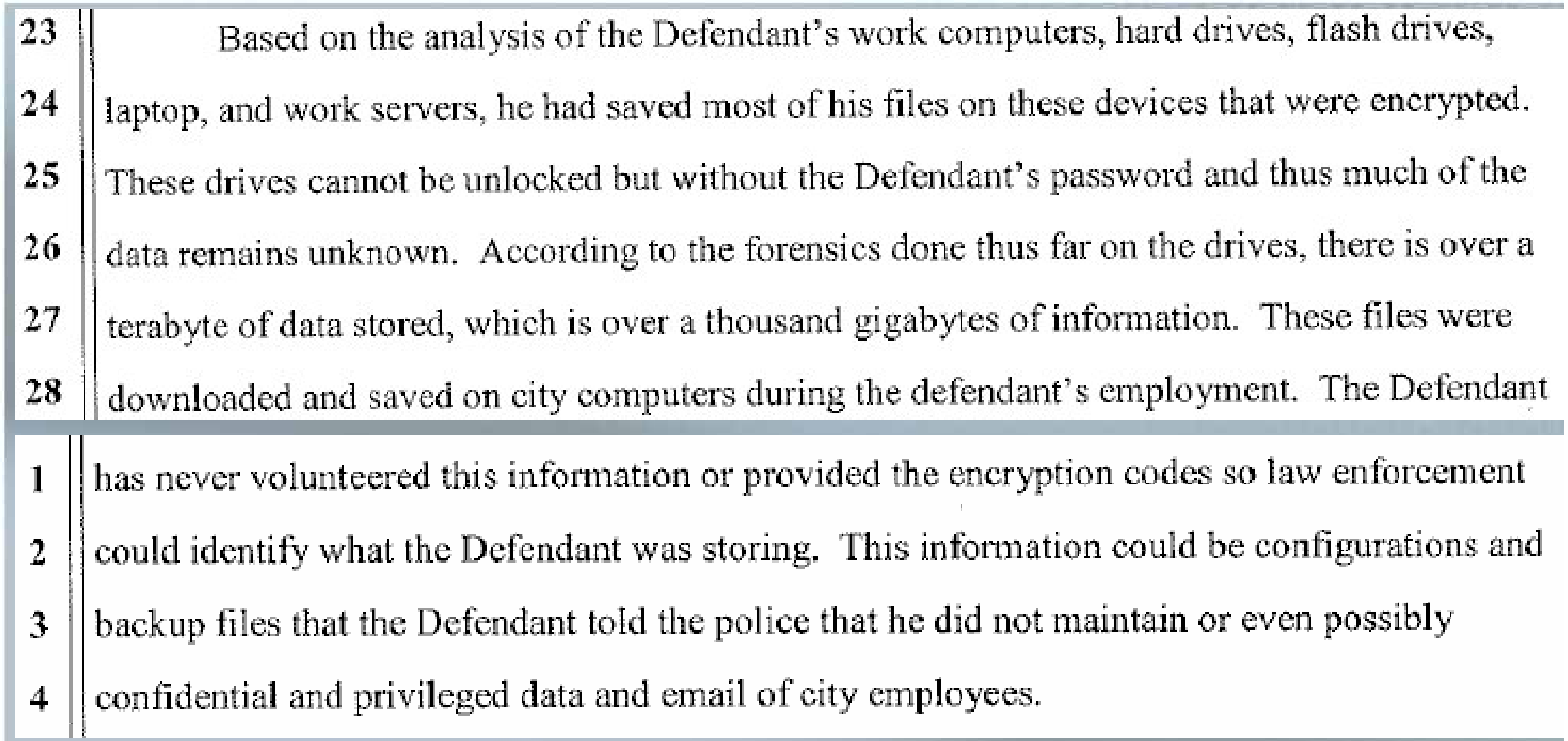
# Putting Terry's List of Passwords In Context

- Privileged system administrators could and can:
  - access any user's files, including things like sensitive email messages, confidential documents, or the shadow password file itself (and with a copy of the shadow password file, one could use rainbow tables or brute force methods to crack passwords)
  - he/she could resurrect "deleted" files from backup tapes or disk snapshots, potentially doing so into a third party's account
  - he/she could create new accounts (including potentially creating accounts for phantom people who don't actually exist)
  - he/she could cache a user's current password,  change it to something new, login and use it, and then change it back
  - he/she can install untrustworthy executables, including trojaned login daemons which might capture passwords

# A Random Observation About The Abuse of Special Administrative Access

- While one would hope that system administrators would be ethical enough to respect the privacy of their users' mail and files, at least one recent survey indicated that up to a third of IT staff admitted to
  - *[…] snooping around the network, looking at highly confidential information, such as salary details, M & A plans, people's personal emails, board meeting minutes and other personal information that they were not privy to. They did this by using their privileged rights and administrative passwords […]*

# Childs's encrypted files



Based on the analysis of the Defendant's work computers, hard drives, flash drives, laptop, and work servers, he had saved most of his files on these devices that were encrypted. These drives cannot be unlocked but without the Defendant's password and thus much of the data remains unknown. According to the forensics done thus far on the drives, there is over a terabyte of data stored, which is over a thousand gigabytes of information. These files were downloaded and saved on city computers during the defendant's employment. The Defendant has never volunteered this information or provided the encryption codes so law enforcement could identify what the Defendant was storing. This information could be configurations and backup files that the Defendant told the police that he did not maintain or even possibly confidential and privileged data and email of city employees.

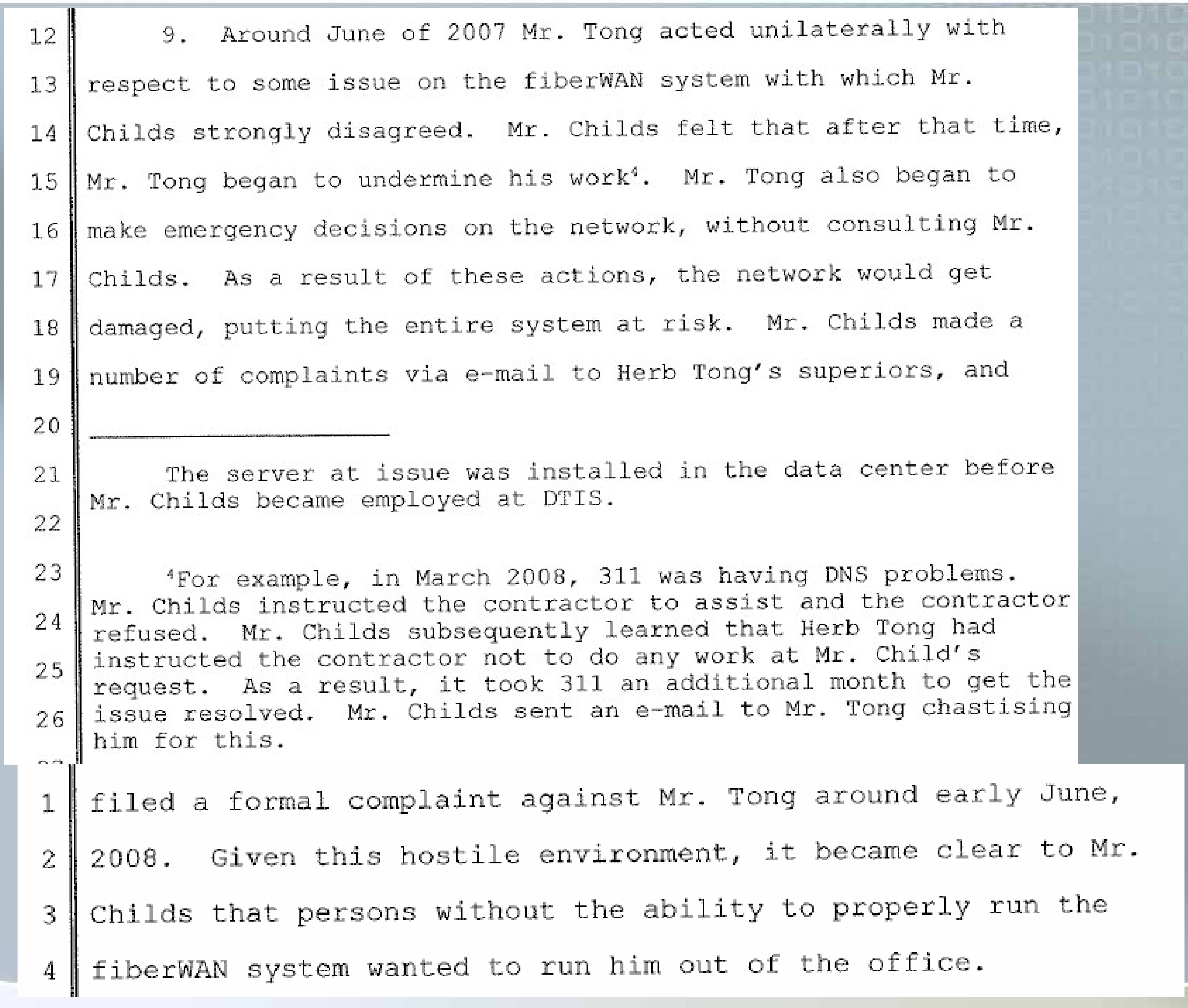
# The General Problem of Disgruntled Employees in Security-Critical Positions

- Imagine that you're an information technology manager, and one of your employees -- who just happens to holds a security-critical job -- has become "disgruntled"/"problematic."
  - What do you do?
  - Leave them in place?
  - Suspend/discharge them?
  - Something else?

# Leadership Inspires Loyalty

- If you're truly a leader, you'll get that loyalty you must rely on.
- As a working proposition, I think there are six types of loyalty:
  - 1. loyalty to the organization as a whole
  - 2. loyalty to the employee's immediate manager
  - 3. loyalty to the customers
  - 4. loyalty to the employee's work friends and colleagues,
  - 5. loyalty to one's work
  - 6. loyalty to one's self.

# From The Defendant's Point of View, What Triggered This Incident?



9. Around June of 2007 Mr. Tong acted unilaterally with respect to some issue on the fiberWAN system with which Mr. Childs strongly disagreed. Mr. Childs felt that after that time, Mr. Tong began to undermine his work[4]. Mr. Tong also began to make emergency decisions on the network, without consulting Mr. Childs. As a result of these actions, the network would get damaged, putting the entire system at risk. Mr. Childs made a number of complaints via e-mail to Herb Tong's superiors, and filed a formal complaint against Mr. Tong around early June, 2008. Given this hostile environment, it became clear to Mr. Childs that persons without the ability to properly run the fiberWAN system wanted to run him out of the office.

The server at issue was installed in the data center before Mr. Childs became employed at DTIS.

[4] For example, in March 2008, 311 was having DNS problems. Mr. Childs instructed the contractor to assist and the contractor refused. Mr. Childs subsequently learned that Herb Tong had instructed the contractor not to do any work at Mr. Child's request. As a result, it took 311 an additional month to get the issue resolved. Mr. Childs sent an e-mail to Mr. Tong chastising him for this.

# Summary of Recommendations

- Take the "insider threat" problem seriously
- Avoid running a large networks with only a single engineer
- Where allowed, conduct background checks and take the result of those inquiries into account when hiring for sensitive positions
- Use scalable AAA practices for large networks, not local passwords on each box
- Insure device configurations have been written to flash or other non-volatile storage so the device can successfully reboot
- Provide adequate physical security for each networked device
- Make backups of configuration files, and routinely store at least one copy with your information security officer
- Subject proposed changes to peer review

# Summary of Recommendations

- Periodically do an external audit of all systems and networks
- Use RANCID to track changes to network device configurations
- Document your network architecture and design, as well as
- common policies and procedures relating to it.
- Monitor your network, including providing an out-of-band
- channel for delivering alerts
- Limit dial-in (or other out-of-band) network access; consider using dial-back modems as an option where access is needed.
- Carefully document locations from which access-limited access is permitted.
- Monitor network traffic with Snort, Bro or a comparable intrusion detection system, and clarify (via policy) who will do this
- Encrypt network traffic end-to-end

# Summary of Recommendations

- Forbid creation of written lists of user passwords
- Forbid privileged access to user files by administrators except for specific permitted purposes, and establish serious sanctions for violations
- Develop institutional policies for dealing with disgruntled/ problematic employees in security-critical roles
- Cultivate leadership skills among IT management
- Cultivate loyalty among IT employees
- Be on the lookout for the development of confrontational situations which may involve security-critical employees
- If a supervisor is the subject of a formal complaint by a subordinate, consider temporarily transferring responsibility for management of that employee to someone else