Physical Security of Advanced Network and Systems Infrastructure

Joe St Sauver, Ph.D.
(joe@uoregon.edu or joe@internet2.edu)
Internet2 Nationwide Security Programs Manager

Joint Techs, Clemson, South Carolina
11:00-11:20 AM, February 1st, 2011

http://pages.uoregon.edu/joe/physical-security/

Disclaimer: all opinions expressed are those of the author

I. Introduction

Do IT Security People Care About Physical Security?

- If you're involved with IT system and network security, it's comparatively common to see security people continually worried about "online" security threats, paying relatively little attention to the physical security of systems and networks. Why?
- One factor may be that we all know the "whole world" can attack our systems and networks online via the Internet, while (in general) attackers need to be locally present to exploit physical security vulnerabilities. As a result, we continually see attacks from online sources, but if we're lucky, we may never have personally experienced a physical attack on IT systems and network resources.
- We may also (incorrectly) view physical security as something that's "someone else's problem" – for example, isn't the physical security of our systems and networks something that the campus police department will take care of? (Maybe, maybe not)

Understanding The Physical Security Risk Model

What Might Happen?

- Accidental damage (e.g., backhoe fade on poorly marked fiber)
- Intentional vandalism (or complete destruction) of facilities
- Theft of hardware (servers, routers, core switches, etc.)
- Loss of system or network integrity (potentially with unauthorized disclosure of PII or other sensitive data)
- Damage from a natural disaster, such as an earthquake

Who Might Do It?

- Random individual (in the accidental case)
- Disgruntled insider (or former employee)
- Financially-motivated criminals
- (Maybe) ideologically-motivated actors (“terrorists”)
- (Or even) state-sponsored professionals (“spies”)

A Couple of Headlines

- **“California Telecom Knocked-Out By Low-Tech Saboteur”**
  April 11th, 2009, http://tinyurl.com/datfv3

  Shortly before 1:30 a.m. on Thursday morning, four fiber-optic cables were severed in an underground vault along Monterey Highway in San Jose, Cal. About two hours later, another four were cut in San Carlos, followed by two more in San Jose shortly thereafter.

- **“Masked thieves storm into Chicago colocation (again!)”**
  November 2nd, 2007, http://tinyurl.com/2pn32z

  The recent armed robbery of a Chicago-based co-location facility has customers hopping mad after learning it was at least the fourth forced intrusion in two years. […] In the most recent incident, "at least two masked intruders entered the suite after cutting into the reinforced walls with a power saw," according to a letter C I Host officials sent customers. "During the robbery, C I Host's night manager was repeatedly tazered and struck with a blunt instrument. After violently attacking the manager, the intruders stole equipment belonging to C I Host and its customers." At least 20 data servers were stolen […]

This is Not Just a Domestic Problem

- **"BT Mayfair phone exchange raided by network hardware thieves leaving customers cut off", September 12th, 2008, http://tinyurl.com/46mfsmf**

  Thieves have broken into a BT phone exchange in London's plush Mayfair and stolen an estimated £2m worth of communications equipment. The theft led to BT business customers and home users in the area being cut off from their phone and broadband internet services. […] They ripped out servers, routers and network cards, which can all fetch a high price on the black market.

- **'Mysterious "Spy" Computer In [Iceland's] Parliament Works Differently Than Being Reported, Tech Expert Says,' January 20th, 2011, http://tinyurl.com/6ja62rq**

  An unmarked computer found in a spare room of [Iceland's] parliament, and connected directly to parliament's internet system, was most certainly planted there […] Any identifying serial numbers had been erased from the machine, nor were any fingerprints found, and its origins have not yet been traced. The police believed that the matter was the work of professionals.

How Does This All Relate to BTOP/US-UCAN?

- The new BTOP US-UCAN network will serve a broader and potentially more sensitive mix of customers than the classic Abilene network or the current Internet2 Network.

- Quoting from the "Notice of Funds Availability" (NOFA) for BTOP Round 2, http://tinyurl.com/yc5m7d5 at page 3797,

> "*Community anchor institutions* ["CAIs"] *means* schools, libraries, **medical and healthcare providers, public safety entities,** community colleges and other institutions of higher education, and other community support organizations and agencies that provide outreach, access, equipment, and support services to facilitate greater use of broadband service by **vulnerable populations**, including low-income, the unemployed, and the aged."

IF Your Customers Include Health Care Facilities or Public Safety, Security Becomes More Important

- For example, natural disasters often can cause network outages. If you're servicing local health care facilities or public safety entities via that down network, local residents who are also affected by that natural disaster may no longer be able to reach emergency responders because of that network outage. Thus, the US-UCAN backbone, and the aggregation networks connecting CAIs to it, may effectively become "life/safety critical" systems.
- Similarly, health-related information and law-enforcement information running over the network may be quite sensitive. Presumably that information would always be protected by strong end-to-end encryption, but given the reality that even access to encrypted traffic can still potentially result in undesirable information disclosure (as a result of traffic analysis, etc.), well, everyone may need to be just a little more careful.

Other Factors

- The BTOP program will result in a substantial amount of new physical facilities (fiber, colo space, network gear, servers, etc.); all those new assets that will also need physical protection.
- The US-UCAN network will be running at very high speeds, and very high speed gear tends to be very expensive. Very expensive assets deserve top notch physical protection.
- The BTOP program will service some difficult/tricky rural locations. That increases the likelihood that it may be hard to at least initially deploy a fully-redundant network architecture
- Federal oversight/review is a given, and the Federal Information Security Management Act (FISMA), includes a variety of physical security-related controls (see PE1-PE19, Appendix F, NIST Special Publication 800-53 Rev 3, http://tinyurl.com/6awxb8d). Even if US-UCAN isn't technically subject to FISMA, federal agencies may still bring a "FISMA perspective" to any security review they do.

Physical Security Areas From FISMA: PE1-PE19

- PE1 Physical and Environmental Protection Policy and Procedures
- PE2 Physical Access Authorizations
- PE3 Physical Access Control
- PE4 Access Control For Transmission Medium
- PE5 Access Control for Output Devices
- PE6 Monitoring Physical Access
- PE7 Visitor Control
- PE8 Access Records
- PE9 Power Equipment and Power Cabling
- PE10 Emergency Shutoff
- PE11 Emergency Power
- PE12 Emergency Lighting
- PE13 Fire Protection
- PE14 Temperature and Humidity Controls
- PE15 Water Damage Protection
- PE16 Delivery and Removal
- PE17 Alternate Work Site
- PE18 Location of Information System Components
- PE19 Information Leakage

Why Should The Folks Here Today Care About This?

- A chain is only as strong as its weakest link (a cliché, but true).
- US-UCAN will likely be built in a way that's quite similar to how the Internet2 network was built: to ensure scalability, the backbone will likely rely on regional aggregators to provide connectivity to individual community anchor institutions [CAIs].
- Therefore, for the system *as a whole* to be secure, we need:
  -- the US-UCAN backbone to be secure, AND
  -- the links between the backbone and regional aggregators to also be secure, AND
  -- the links between the regional aggregators and the CAIs to also be secure.
- **Securing the network will thus require the participation and cooperation of regional aggregators. Many of those regional aggregators are present here in the audience today.**
- So what physical security vulnerabilities should you worry about?

II. Physical Security Vulnerabilities

You Can't Worry About Everything…

- In the real world, we all have to "make our numbers," and that usually means prioritizing and only spending money on security measures when it is necessary and cost effective for us to do so.
- The risks that you or I perceive may be different than the risks that someone else sees under different circumstances. For example, a military unit in Iraq or Afghanistan might devote considerable attention to protecting facilities from attack by vehicle borne improvised explosive devices (VBIEDs), their #1 threat.
- Here in the United States, higher education might largely discount that particular threat, choosing to "accept" that risk rather than making investments in anti-VBIED technologies such as physical standoff zones, blast resistant glazing, vehicle inspection stations, etc. [Of course, in thinking about such a choice, incidents like the May 1st, 2010, attempted bombing in Times Square, or the attempted Christmas Tree bombing in Portland, make you wonder]

1) Fiber Cuts

- Regardless of how skeptical we may be of any other physical security threat, one very real threat that I think we're all willing to acknowledge is that backhoes and other heavy equipment have an uncanny ability to find and accidentally cut buried fiber.
- You can help minimize the risk of unintentional damage to buried fiber by taking appropriate steps, including insuring that:
  -- all buried facilities are well-documented as actually constructed
  -- easily visible "buried cable" posts or signs are installed where appropriate or required
  -- you (or your service agent) subscribe to your state's call-before-you-dig one-call utility notification center, and you make timely response to all relevant locate-and-mark requests
  -- any non-conductive/otherwise hard to locate facilities are buried with a tracer wire or conductive marking tape (this may be a legal requirement in some states, e.g., ORS 952-001-0070)

The Downside of Transparency

- At the same time we recognize and accept the need to be transparent about where fiber is located in an effort to avoid the problem of accidental fiber cuts, potential bad guys might also be interested in our fiber deployments. For example:

  -- Are there critical choke points, such as bridges across major rivers or tunnels through large mountain ranges, where virtually all fiber follows a common path out of necessity?
  -- Are there unmonitored access points (manholes, hand holes, fiber pedestals, etc.) where an attacker might be able to gain access to your fiber without being detected?

- Obviously you need to balance the need to provide enough information to avoid accidents, while simultaneously avoiding giving your enemies a “blueprint” for how to best attack you.

Architecting and Building for High Availability

- One way you can improve the physical security of your network is by adding redundancy, excess capacity, and resiliency to it.
- Your network should be architected and constructed so that there are no choke points or "single points of failure" -- loss of any single link or piece of gear should NOT result in an outage! Think, "We must always have redundant paths over diverse facilities!"
- Moreover, you must also have enough spare capacity on failover links so that if you do end up needing to actually use them, they won't be congested (or you need a plan to selectively shed load).
- You also want to work to ensure that if an outage does occur, you can recover from it in a timely fashion. For example, are you continually monitoring your network and maintaining adequate local spares?
- Of course, the downside of all this is that high availability comes at a cost ("you can get whatever level of availability you can afford").

Diminishing Returns

- When you're thinking about how much you want to spend to insure that your network is "always available," you need to remain cognizant of the law of diminishing returns.
- The first backup/failover circuit you add will likely provide a substantial improvement in system availability, since if your main production circuit fails, that backup circuit will save your bacon. It likely represents a good bit of insurance for you to buy.
- If you're really risk averse or your service must absolutely remain available, a second backup/failover circuit might allow you to avoid an outage in the rare circumstances where both your primary and your secondary circuits simultaneously experience an outage – but, that *should* be a vanishingly rare event.
- But what of a third or fourth or n'th backup/failover circuit? You might only need that extra circuit one time in ten million, and the cost of eliminating an event that rare may be prohibitive.

2) Network Confidentiality and Fiber Taps

- As the network begins to carry potentially sensitive health care related traffic or classified traffic from public safety agencies, traffic confidentiality will become more important.
- You may want to proactively and continually monitor your network links for any brief outages (which might be associated with the introduction of splitters or other unauthorized network elements). At the most basic, this can be done by sending/ continually monitoring an ongoing “heartbeat” signal.
- More sophisticated units (as used to protect federal classified networks such as SIPRNet and JWICS), are also available if appropriate (see http://www.networkintegritysystems.com/)
- You may also want to periodically characterize your deployed fiber with an OTDR (optical time-domain reflectometer) to identify any “unexpected physical anomalies” which may have “developed.” (Macrobends may be enough for data interception)

Live Open Ethernet Jacks/Ports

- It is amazing how often organizations will tolerate live open ethernet jacks/ports to which random people can plug in systems. Sometimes this even includes unlocked wiring closets, or publicly touchable routers, switches, or other network equipment.
- Most universities do not allow "free love" open wireless networks, so why would you allow anyone with an ethernet cable to have open access to your wired network? Some options to consider:
  -- only heat up jacks on request, or at least disable jacks in hallways and empty offices by default
  -- require authentication for most physical ethernet connections the same way you do for wireless connections
  -- consider locking unused jacks and installed patch cables (e.g., see www.rjlockdown.com, but remember that Torx screwdriver bits are publicly available and recognize that jack plates can still be removed or patch cables cut and reterminated for access)

3) The Security of Cabinets, Rooms and Buildings

- When we think about the physical security of networks, there's a temptation to think just about *the network*, e.g., the fiber and the ethernet themselves.
- In reality, every network also has numerous other physical facilities (cabinets, rooms, buildings, etc.) housing things like key network equipment (optronics, routers, switches, etc.), as well as servers, critical staff, documentation, media, etc.
- Those facilities also need to be physically secure.
- Often that physical security begins with access control via locks.
- Naturally, we all know that the locks on data equipment cabinets typically aren't very strong, and more often than not the keys for those cabinet are just left on top of the cabinet so they don't get lost, cough, but because locks are used so many places related to computing and networking, let's start by talking about locks.

Traditional Pin Tumbler Locks

- Even though traditional pin tumbler locks have well known limitations, they still form at least part of the physical security at most sites, including many computer or networking sites.
- It is not my intention to provide a tutorial for intruders, but if you think that traditional pin tumbler locks provide anything even *remotely* approaching reasonable security, I'd urge you to Google for the phrase "bump key" and do a little reading.
- If discovery of an intrusion isn't a problem, you should also know that many traditional locks can be drilled, pried, ground, frozen or otherwise defeated by brute force in just a matter of minutes.
- Thus, for any lock that "matters," you should probably consult with a professional locksmith and have a high security lock (such as those made by Medeco) installed, reinforcing the door and the door jamb (including the strike plate area) at the same time.
- Don't forget to secure any external door hinges, too!

Padlocks

- Padlocks are widely used to secure network equipment. They are typically subject to all the issues associated with traditional pin tumbler locks, but they have additional issues of their own:
  -- warded padlocks (see image at right) are trivial to open; they should **NEVER** be used
  -- some padlocks are stamped with their "key code;" if you don't remember to remove that code, it may be possible to use those numbers to create or find a key for that lock
  -- the unshielded shackle of a padlock can often be cut with bolt cutters or a torch
  -- even if you have a padlock that's secure, it may be used in conjunction with a weak and easily defeated hasp or chain (ugh)

- The ultimate? The Navy has approved the S&G 951C High Security Padlock, but at ~$1,350/lock, it might be, um, a little pricey

Keys

- Key-related issues are another reason why traditional locks often provide mediocre security.
- In a university environment, it is routine for the same key to get issued to multiple people. When one of those keys get lost (or is not recovered when someone quits or is terminated), the locks that are opened by that key tend not to get rekeyed (typically, the cost of doing this would be prohibitive, and there are only a finite number of usable key combinations given physical constraints).
- Many sites also use master keys, allowing supervisors or custodial staff to have access to all offices on a given floor or in a particular building. If control over a master key is even temporarily lost (or an intruder can gain access to lock cylinders from multiple doors using the same master key), the intruder may be able to make a duplicate master and have the run of your facility.
- You really want to have a conversation with your lock & key person

Alternatives to Locks and Keys

- Many facilities have moved to key cards (swipe cards, prox cards, etc.) and/or biometrics as an alternative to traditional locks & keys
- Key cards offer distinct advantages over traditional keys:
  -- key cards can be integrated into user site IDs/badges
  -- key card use can be tracked, while use of a key leaves no audit trail or record
  -- key cards can be programmed to work only during particular days or particular periods of time, while keys work all the time
  -- many key card systems can be configured to require "two factors" (e.g., you must use your key card AND enter a PIN code)
  -- upon termination, a key card can be instantly canceled with no need to manually rekey the system, etc.
- Biometrics are another alternative for particularly high security facilities, however relatively high costs, false negatives, and user acceptance issues still limit their deployment.

Building Security:
Piggy Backing/Tailgating/Stay Behinds

- Key cards or biometrics won't help if random individuals can gain access to a secure facility by piggy backing/tailgating behind an authorized user. Floor to ceiling turnstiles or mantraps (interlocking pairs of doors) can be used to control this phenomena, or an attendant at the door can also ensure that everyone coming in "cards in" as required (but I know that this is something that many higher education sites fail to enforce).
- There's also the potential problem of "stay behind" visitors – if you're not continually escorting all visitors from entry to exit, or at least signing all visitors in and out, how do you know that all visitors who've entered your facility have left by the end of the day? An unescorted and forgotten visitor can be the "camel's nose" that defeats many of your physical access controls, potentially allowing anyone or everyone to gain access to your facilities.

Walls, Ceilings, Floors, Roofs, Utility Tunnels, Etc.

- Sometimes you'll see a high security lock on a high security door "protecting" a room with externally accessible glass windows, sheetrock walls, a suspended ceiling, and maybe even a raised floor.
- In that sort of environment, an intruder can ignore the high security lock and the high security door, and just break the window, or punch through the sheet rock walls, or climb in via the suspended ceiling or raised floor. (Embedded heavy gauge wire mesh can at least make that sort of through-the-wall or through-the-ceiling or floor entry more difficult)
- Similarly, have you secured your roof? Or could someone use a ladder to get to your roof, and then go through an unsecured roof hatch or skylight?
- What about any utility tunnels? Manholes are often one of the easiest-to-breach access points. Although locking manhole covers are available (e.g., see www.securemanholes.com), most manhole covers are simple cast iron units that provide no impediment to an intruder with a manhole cover lifter (or just a couple of bolts and some wire).

Fencing, Obstacles, Intrusion Detection, Landscaping

- University campuses aren't like industrial or government facilities, but if you can add a fenced perimeter around critical facilities, that immediately adds significantly to your site's physical security.
- Government and military folks (who do worry about things like VBIEDs) like a wire cable-reinforced perimeter fence that's ideally at least fifty feet away from the facility that's protected, built from 9 gauge (or heavier) chain link, seven feet tall, with an outward facing razor wire top guard plus a bottom rail, well anchored and backed up by things like interlocking precast concrete obstacles or large concrete planters. Dual fence designs are also popular.
- Any sort of fence will at least serve to create a public exclusion zone in which an intruder can be readily identified and intercepted for questioning. Extensive lighting plus physical intrusion detection systems will help managing that exclusion zone, and obviously any landscaping should not provide hiding spots for intruders.

Example of a Fencing Failure

- "A fence approximately six feet high surrounds some of [the Kinshasa Nuclear Research Center] CREN-K. The fence is constructed of cement in some places and chain-link in others. The fence is not lit at night, has no razor-wire across the top, and is not monitored by video surveillance. There is also no cleared buffer zone between it and the surrounding vegetation. There are numerous holes in the fence, and large gaps where the fence was missing altogether. University of Kinshasa students frequently walk through the fence to cut across CREN-K, and subsistence farmers grow manioc on the facility next to the nuclear waste storage building. […] No fence separates the nuclear waste storage building and the University of Kinshasa's women's dormitory. The two buildings sit approximately 300 meters apart, and one can walk freely from one to the other across the manioc field." http://tinyurl.com/68sgdds

Alarms and Guards

- Access control features such as locks and reinforced doors and walls can't keep a determined intruder out "forever" – virtually any facility can eventually be breached if the intruder has enough time and no interruptions.
- What access control features do give you is a window of time for guards to respond and deal with any intrusion attempt.
- The sooner your guards know that someone is attempting to break in, the more time they'll have to mobilize and deal with the attempted intrusion. Alarms buy you that response time.
- Again, just as was the case with locks, you should consider engaging an alarm professional to help you plan and deploy a suitable comprehensive alarm system (including things like area motion detectors, and perimeter integrity alarms with window-ajar and door-ajar sensors). You should also review response requirements with campus police and municipal law enforcement.

Surveillance Video

- You can't be everywhere at once, so take advantage of surveillance cameras to increase your security leverage. Cameras have come way down in price, while quality has gone up (as has ease of installation). It should now be possible for you to affordably add surveillance video throughout critical installations.
- Surveillance video may deter issues from arising in the first place: if people know they're potentially being monitored, that alone may deter them from engaging in illegal activities.
- If illegal activities do occur, surveillance video can provide crucial evidence documenting what happened during the incident: (a) When did the incident occur? (b) How did the incident occur? (c) Who did it? (d) What did they take/what did they do?
- Consider using a redundant out-of-building digital video recorder to ensure that an in-building video recorder doesn't get stolen or compromised during a security incident.

4) Emergency Systems: Fire Detection & Suppression

- Electrical fires are one of the most destructive events an IT organization can run into, and fire suppression has become trickier since new inert gas ("Halon 1301") installations have been banned due to ozone depletion effects.
- Automatic water sprinkler systems ("dry pipe" systems) are the most common alternatives, but water sprinkler systems may not be effective when it comes to suppressing electrical fires occurring in machine rooms under raised floors.
- Non-Halon gaseous fire suppression systems (for example, carbon dioxide based systems) may be an alternative, but they represent serious potential risks for operators and other personnel who may need to be rapidly evacuated in the event of a fire. See the discussion of some alternatives at http://tinyurl.com/6agevle
- Note: regrettably, not all fires will take place in your well-fire-suppressed machine room…

OSU's Thanksgiving 2010 Steam Tunnel Fire

- "Oregon State University resumes classes, though some phone and computer services still disabled from fire," November 29th, 2010, http://tinyurl.com/5sxxx3c [emphasis added below]

> Some Oregon State University buildings still had not regained telephone or computer data service Monday as the result of an electrical fire last week, but all classes resumed normally. The fire erupted early last Wednesday morning in wiring that runs through the university's steam tunnels, 6-to-8-foot-tall tunnels that run under most buildings on campus. Electrical wiring, telephone lines and **fiber optic cables** thread through the tunnels along with wrapped steam pipes that carry heat to buildings. Investigators are still trying to determine what caused an arc flash – a burst of electrically charged energy that burns at a temperature of 5,000 degrees or higher. The arc singed sections of wiring extending about a 100 feet from the flash point in three directions, said Vincent Martorello, director of facility services. The university gave its nearly 24,000 students early dismissal for the Thanksgiving break on Wednesday morning because the fire had disabled fire alarms in some buildings, Simmons said. The fire did not affect dormitories, **but it left five buildings Monday without computer data connections** and a dozen buildings without telephone service. Telephone service may not be fully restored until the end of the fall term, university officials said.

Source: http://tinyurl.com/65mrh3w

Emergency Power and Cooling

- Often uninterruptible power supplies prove to be too small for the load they've been stretched to support. In those cases, even if you immediately began shutting down systems as soon as the power flipped to the UPS, you would not be able to cleanly take down all the covered equipment before running out of juice (and naturally most people don't want to begin powering things down until they're SURE that they're not facing just a brief outage). Check and figure out how long you can run with your actual load.
- UPS systems need to be backed up by diesel generators. Have you tested yours recently? How much fuel do you have available for it? In an emergency will you be able to get more? Are you sure?
- While most sites worry about emergency power, many forget to think about emergency cooling. If your machine room is going to overheat, even if you have juice, you won't be able to stay online. Spend some time thinking about your emergency cooling plan.

Network Operational Continuity in a Disaster

- Would your network continue to operate if your primary network operations center was hit by a major disaster, such as an earthquake?
- We can tease apart two issues here:
  -- Will you have a functional NOC, post-disaster?
  -- And will your remote network equipment continue to operate?
- These days, realistically speaking, you will likely want full replication of your NOC at an out-of-region location if you want to be able to continue to operate your network after a major disaster.
- That replicated NOC will need both trained and ready-to-go network engineers and NOC staff, as well as replicated servers and live current copies of all NOC databases. We recognize that this is a potentially expensive proposition, but one that we think deserves serious consideration.

Disaster Continuity for Remote Gear, Including Emergency Out-Of-Band Access

- A major disaster, such as an earthquake, may also directly impact remote network equipment. Don't forget to plan for the emergency power, cooling and remote access needs of your remote networking sites.

- Every installation with active electronics needs, at a minimum, its own emergency power and cooling, particularly if primary power is coming from only a single utility feeder, or utilities for a remote site are aerial rather than buried.

- It may also be worth spending some time thinking about how you will securely handle emergency out-of-band access to remote gear if in-band access is interrupted due to a network outage.

5) Miscellaneous Items: Personnel Controls

- Personnel vetting and related controls are often viewed as a key part of physical security because on-site personnel enjoy unique physical access to site facilities.
- Historically universities have rarely done background checks on their employees, however, that practice has been evolving over time, particularly for system and networking staff members having effectively unlimited access to the University's infrastructure.
- As staffs are beefed up to support BTOP/US-UCAN activities, don't neglect personnel background checks in your eagerness to fill some of those hard-to-fill positions!
- Be sure to discuss any planned background checks with your Human Resources Department, since specific notice and consent requirements or other limitations may apply.

Outputs: Dumpster Diving and Surplus Equipment

- Historically, many crackers got their start by fishing interesting computer and networking gear out of corporate dumpsters (a fine art normally known as “dumpster diving”). Even today, it is still important to pay attention to how you handle your trash.
- Today, there’s much more emphasis on recycling, and that’s laudable, but any storage media in surplus equipment needs to get wiped before that gear gets sold or otherwise disposed of, and sensitive documents need to be shredded or sequestered in a confidential document disposal container for approved disposal.
- Speaking of confidential document disposal containers, it is routine for those “wheelie” cans to live in mailrooms or corridor areas, locked to prevent browsing of discarded confidential documents, but often not living chained down. Presumably the unauthorized removal of a full confidential document disposal container would be a disconcerting event, so be careful!

All The Rest

- It isn't possible to go over everything that we really should talk about when it comes to IT physical security in only twenty minutes, so please don't think that this is a comprehensive treatment –it's not. This talk is really just designed to "wet your whistle" when it comes to thinking about physical security.

- If you're not routinely talking about physical security at your site, or you don't have a formal physical security policy, you may want to think about forming a group to focus on this important area. Hopefully this talk will at least provide some starting points for that conversation.

Thanks for the Chance to Talk!

- Are there any questions?