

Physical Security: A Crucial (But Often Neglected) Part of Cybersecurity

Joe St Sauver, Ph.D.

(joe@uoregon.edu or joe@internet2.edu)

Internet2 Nationwide Security Programs Manager

Eugene IT Pro Forum

Eugene City Brewery, 21 June 2011, 6:30PM

<http://pages.uoregon.edu/joe/eugene-it-pro-forum/>

Disclaimer: all opinions expressed are those of the author

I. Introduction

Welcome and Thanks For Participating Today!

- Welcome to the Eugene IT Pro Forum at the Eugene City Brewery! What a great location for this meeting!
- I'd particularly like to thank Quentin Hartman for the invitation to speak with you tonight.
- Mindful of the fact that this is an "after work" talk, and you all are enjoying fine beverages, I'll do my best to keep this talk moving right along.
- In particular, Quentin has already stressed that I've got an hour (at the most). **I promise I won't run over!**
- I also wanted to explain, for those of you who may not be familiar with my slide style, that I normally do fairly detailed slides to help those who may look at this talk after the fact, the hearing impaired, and Google. **A second promise to you: I won't just read my slides to you!**

Helping the Good Folks, Not the Bad Ones

- Any time you talk about security issues, you need to walk a careful line: you want to help the good folks identify and fix security issues they may be facing, but you don't want to give the bad guys (or bad gals) inspiration or practical tips.
- (I think) this talk threads that needle.
- You'll notice that I will usually carefully cite a public source for pretty much anything I share with you tonight, so none of this should be information that's new or particularly helpful to the bad folks.
- At the same time, we may talk about some issues you haven't thought about much...

Physical Security and IT:

It's Not A Cool Topic, I Know, I Know

- Physical security of systems and networks is probably the last topic you wanted to hear about tonight.
- We could have talked about a lot of things that are more "trendy," I suppose, such as the **security of mobile devices**,* but I do think that the physical security of systems and networks is a pretty important (if largely underappreciated) area.
- Oh heck, maybe we are talking about things like the security of mobile devices, at least if "mobile devices" includes laptops...

* "Securing Mobile Devices: A Security Professionals 2011 Pre-Conference Seminar,"

<http://pages.uoregon.edu/joe/securing-mobile-devices/>

II. Losing Hardware (Maybe Containing PII)

A Recent Example from the UK Press

Story URL: <http://www.zdnet.co.uk/news/security-management/2011/06/15/nhs-laptop-loss-could-put-millions-of-records-at-risk-40093112/>

NHS laptop loss could put millions of records at risk

By Jack Clark, [15 June 2011](#) 15:26

NEWS

A laptop containing unnamed patient information has gone missing from a subsidiary of the NHS North Central London health authority, putting the privacy of patients at risk.



A laptop containing unnamed patient information has gone missing from a subsidiary of the NHS North Central London health authority. Photo credit: [comedy_nose/Flickr](#)

[The Sun reported on Wednesday](#) that the laptop, which was lost along with 19 others three weeks ago, contained the unencrypted health details of over 8.63 million people and records of 18 million hospital visits, operations and procedures. It was taken from a storeroom of [London Health Programmes](#), a medical research organisation based within the NHS North Central London health authority.

Some Things to Note About That Incident

- This incident happened **just last month**.
- It potentially impacts **millions of people**.
- The incident didn't involve a sophisticated attack – **it took place because a laptop was able to be stolen from a storeroom**.
- Even though laptop whole disk encryption (WDE) is a best common practice (BCP) these days, **the laptop's hard drive apparently wasn't protected by WDE**.
- I'd also would wager those laptops didn't have stolen laptop locator software (such as "Lojack") installed on them.
- The article goes on to say, "All the laptops were password protected, and our policy is to manually delete the data from laptops after the records have been processed."
- Hmm. "All the laptops were password protected." Does a password **really** protect the contents of missing laptops?

Physical Access Typically Equals Total System Control

- Sometimes people think that they've "protected" a device (such as a laptop) because it has been made to require a boot-time (or "BIOS") password before it will boot its operating system.
- That's a mistaken impression.
- Remember, if an attacker has physical access to your system, he or she can remove the hard drives and mount it on another system that they control.
- At that point they can mount and access any unencrypted files on your hard drives at will, even if the original system was using a hardware system startup password.
- But what if that laptop HAD also been using whole disk encryption?

Encryption Isn't a "Magic Bullet," Either, Unfortunately

- When correctly used, carefully-implemented whole disk encryption is something that only a national-level intelligence agency could successfully attack using technical crypto-analytical means.
- However, any halfway competent private investigator with physical access could install a commercially available hardware key logger (or even just use a hidden camera to watch the user's screen and keyboard!), and once s/he has the user's passphrase, s/he could easily defeat that whole disk encryption scheme.
- And let's not even mention so-called "rubber hose cryptography!"
- So I would argue that physical security can genuinely matter! Far better to ensure that bad people can never get near a laptop in the first place, rather than having to worry about WDE failure modes, right?

Desktops Can Be As Vulnerable As Laptops

- Somewhere along the line, many folks began to focus all their workstation security efforts on laptops, effectively ignoring desktop workstations. That's a bad idea, because desktops can be just as vulnerable, including being at risk of potentially having hard drives (sometimes with unencrypted PII!) stolen.
- If you've ever run an unattended computer lab, you may be familiar with lab users defeating hardware security devices to steal system components. It can be quite tricky to fully secure all parts of modern systems (including small parts such as memory, and peripherals such as keyboards, mice, power bricks, and even cables – you'd be amazed at what people will steal, or try to steal).
- You may be able to indelibly engrave ownership information on some property (or you can try STOP plates), but often only 100% positive user identification backed up by a video record of activity in the facility will stop theft of desktop systems or components.¹¹

Some HW Protective Solutions Can Be Expensive

- If a new low-end PC costs \$500 or less these days, it can be frustrating if you need to spend half that much (or more!) on top of that amount to buy a hardware security enclosure to lock it down.
- Some hardware enclosures may make access for routine maintenance more difficult.
- It may help to remember that you're not really protecting the \$500 PC with the enclosure you buy, but rather the hundreds of thousands or millions of dollars worth of PII that's contained in the system (even though you're also being good about backing that information up, and encrypting it, right?)
- There's also perception issues involved: have you taken REASONABLE common steps to protect your assets? (Would cheaper security cables be equally acceptable for this purpose?)

This Isn't "Just About Workstations" -- Another Physical Security Incident: Theft of Backups @ ECMC

Incident Recap

- Physical theft of two 200-lb safes from a locked room in our secured headquarters.
- Safes included DVDs containing PII data on 3.3 million student loan borrowers.
- Data recovered within 36 hours (although ECMC was not notified for nearly 1 month).
- Significant cost.
- Significant impact.

www.ifap.ed.gov/presentations/attachments/50DontBeTomorrowsHeadlinesV1.ppt

(Reportedly, the stolen safes were small consumer-sized units, and were wheeled out on rolling office chairs...)

Some Things to Note About This Incident

- If you have applied for a student loan for yourself (or for a family member), you know how many details you have to provide – it would truly be unfortunate for that sort of detailed financial PII to end up getting compromised.
- This was yet another incident potentially impacting **millions of us**
- The incident didn't involve a sophisticated attack – **it took place because backups were able to be physically stolen.**
- Do you think the thieves might have hoped those safes had cash? Should they have been clearly labeled, "Contains No Money"?
- And could those safes have been better secured? For example, given how light and easy to move they seem to have been, could they have been blind-bolted down to a concrete floor perhaps?
- I also wonder: were the backups in the safes encrypted? (I bet not – they were "securely" ensconced in safes, after all, right?)

Please Note, I Do NOT Mean to Discourage Backups!

- Backups are a very important part of physical information security. I do NOT mean to discourage anyone from routinely doing them!
- However, when doing backups:
 - make sure you encrypt them (while ensuring that the right people know password to decrypt those backups if they need to do so!)
 - make sure the backups aren't just thrown on a shelf somewhere, store them securely offsite!
 - don't reuse backup media – use fresh media each time, or at least rotate your backup media
 - confirm that you're actually able to restore stuff from your backups! If there's a problem with them, you want to know now, not when you're desperately in need of what's on that unusable media.

"4800 Aussie Sites Evaporate After Hack"

[* * *]

In a **statement** published today, Distribute.IT said it had been working around the clock in an attempt to recover data from its affected servers.

"At this time, We regret to inform that the data, sites and emails that were hosted on Drought, Hurricane, Blizzard and Cyclone can be considered by all the experts to be unrecoverable," it said.

"While every effort will be made to continue to gain access to the lost information from those hosting servers, it seems unlikely that any usable data will can be salvaged from these platforms.

"In assessing the situation, our greatest fears have been confirmed that not only was the production data erased during the attack, but also key backups, snapshots and other information that would allow us to reconstruct these servers from the remaining data."

The company said 4800 websites were affected and since it did not have the capacity to transfer the domain names to other parts of its platform, Distribute.IT had no choice "but to assist you in any way possible to transfer your hosting and email needs to other hosting providers".

The significant data loss has raised questions from backup experts as to why Distribute.IT did not appear to have offsite backups of customer data.

[* * *]

Sometimes They "Take," Sometimes They "Give"...

- **"Stuxnet Worm Heralds New Era of Global Cyberwar," www.guardian.co.uk/technology/2010/sep/30/stuxnet-worm-new-era-global-cyberwar**

The memory sticks were scattered in a washroom at a US military base in the Middle East that was providing support for the Iraq war. [...]

The result was the delivery of a self-propagating malicious worm into the computer system of the US military's central command – Centcom – which would take 14 months to eradicate.

- **‘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.

Hardware With PII Isn't The Only PhysSec Issue

- “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 tazed 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** [...]

- “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.

Not All Incidents Are Intentional: Fiber Runs Across Bridges, and Bridges Sometimes Fall Down -- The I-35 Bridge, St Paul MN, August 1st, 2007



26 Sec. Video: http://www.youtube.com/watch?v=EKLjB_nq76c

Fiber Also Runs Through Tunnels; Tunnels Sometimes Accidentally Burn: The Howard St Tunnel Fire, Baltimore, July 18th, 2001



Image: www.baltimoresun.com/features/bal-trainfiregallery,0,1855948.photogallery

See also section 3.4.1 of http://ntl.bts.gov/lib/jpodocs/repts_te/13754.html

Tunnels Like The Howard Street One Can Be Key Physical Security Choke Points

A Silicon Valley company that tracks Internet traffic said Wednesday's train accident caused the worst congestion in cyberspace in the three years that it has monitored such data.

The link through Baltimore "is basically the I-95 of Internet traffic into and out of Washington," said Bill Jones, director of public services for Keynote Systems Inc. of San Mateo, Calif. This week's accident caused more disruption than an incident last winter when an act of sabotage against Microsoft Corp. tied up networks, he said.

The company, which monitors Internet flow by the hour on its Web site, said that the accident had almost no impact in some areas, including parts of Baltimore, while certain connections were 10 times slower than normal, such as the ones between Washington, D.C., and San Diego.

"There was a ripple effect around the country with corporate networks due to this Baltimore disaster," said Frank Stanton, an executive with Lexent Inc., a New York-based company that repaired fiber-optic cable after the World Trade Center bombing in 1993. "Everybody thinks they have redundancy, but these type incidents show people there are huge issues. When you cross rivers and bridges, these choke points are the Achilles' heel."

Source: http://articles.baltimoresun.com/2001-07-21/news/0107210195_1_fiber-pratt-st-internet-traffic

Bad As Those Incidents Are, Others Are (Arguably) Worse



New cable cut compounds net woes

A submarine cable in the Middle East has been snapped, adding to global net problems caused by breaks in two lines under the Mediterranean on Wednesday.

The Falcon cable, owned by a firm which operates another damaged cable, led to a "critical" telecom breakdown, according to one local official.

The cause of the latest break has not been confirmed but a repair ship has been deployed, said owner Flag Telecom.

The earlier break disrupted service in Egypt, the Middle East and India.

"The situation is critical for us in terms of congestion," Omar Sultan, chief executive of Dubai's ISP DU, told The Associated Press, following the most recent break.

Wednesday's incident caused disruption to 70% of the nationwide internet network in Egypt on Wednesday, while India suffered up to 60% disruption.

<http://news.bbc.co.uk/2/hi/7222536.stm> , October 4th, 2008

Summarizing The Physical Security Risk Model

What Might Happen?

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

Summarizing The Physical Security Risk Model

Who Might Do It?

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

III. Is Physical Security Something That's On The IT Security Radar?

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 threats over the wire, 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 our local security guards will take care of? (Maybe, maybe not)

Physical Facilities Security Is Certainly A Big Issue for Federal Agencies (But They're Generally Not Going to Share Their Thinking With Us!)

http://www.dhs.gov/files/committees/gc_1194978268031.shtm

Interagency Security Committee Standards and Best Practices

The ISC's mandate is to enhance the quality and effectiveness of physical security in, and the protection of buildings and civilian federal facilities in the U.S. The ISC standards apply to all civilian federal facilities in the U.S.—whether government-owned, leased or managed; to be constructed or modernized; or to be purchased.

Government users with a need to know may access the Interagency Security Committee standards that are For Official Use Only (FOUO). To request access, please send an e-mail to ISC@DHS.gov with your full name and contact information including e-mail, the name of your agency, and the reason you need access.

Standards

2011/Design-Basis Threat Report (FOUO): Creates a profile of the type, composition, and capabilities of adversaries. It is designed to correlate with the countermeasures contained in the *Physical Security Criteria for Federal Facilities*. In order to keep pace with the changing nature of the threat to federal facilities, updates to the DBT are made every six months, and a full membership review of the document will be conducted annually.

2010/Physical Security Criteria for Federal Facilities (FOUO): Establishes a baseline set of physical security measures to be applied to all federal facilities and provides a framework for the customization of security measures to address unique risks at a facility. These baseline measures provide comprehensive solutions in all five areas of physical security, including site, structural, facility entrance, interior, security systems, and security operations and administration.

2009/Use of Physical Security Performance Measures: (PDF, 16 pages - 631 KB) New ISC policy requires all federal agencies to assess and document the effectiveness of their physical security programs through performance measurement and testing. This standard provides guidance on how to establish and implement a comprehensive measurement and testing program.

2008/Facility Security Level Determinations (FOUO): Defines the criteria and process to be used in determining the facility security level of a federal facility, a categorization that then serves as the basis for implementing ISC standards.

One Notable Federal Exception: FISMA

- The Federal Information Security Management Act (FISMA) information security standards includes a variety of physical security-related controls (see PE1-PE19, Appendix F, NIST Special Publication 800-53 Rev 3, <http://tinyurl.com/6awxb8d>).
- I'm not normally a huge FISMA cheerleader, to say the least, but in this case, the FISMA authors should be commended for at least being willing to share their thinking with us.
- FISMA specifically calls out **19** areas related to physical security, areas that you might want to keep in mind as we talk tonight...

Physical Security Areas From FISMA: PE-1—PE-19

- PE-1 Physical and Environmental Protection Policy and Procedures
- PE-2 Physical Access Authorizations
- PE-3 Physical Access Control
- PE-4 Access Control For Transmission Medium
- PE-5 Access Control for Output Devices
- PE-6 Monitoring Physical Access
- PE-7 Visitor Control
- PE-8 Access Records
- PE-9 Power Equipment and Power Cabling
- PE-10 Emergency Shutoff
- PE-11 Emergency Power
- PE-12 Emergency Lighting
- PE-13 Fire Protection
- PE-14 Temperature and Humidity Controls
- PE-15 Water Damage Protection
- PE-16 Delivery and Removal
- PE-17 Alternate Work Site
- PE-18 Location of Information System Components
- PE-19 Information Leakage

An Example: PE-4 – Access Control for Transmission Media

PE-4 ACCESS CONTROL FOR TRANSMISSION MEDIUM

Control: The organization controls physical access to information system distribution and transmission lines within organizational facilities.

Supplemental Guidance: Physical protections applied to information system distribution and transmission lines help prevent accidental damage, disruption, and physical tampering. Additionally, physical protections are necessary to help prevent eavesdropping or in transit modification of unencrypted transmissions. Protective measures to control physical access to information system distribution and transmission lines include: (i) locked wiring closets; (ii) disconnected or locked spare jacks; and/or (iii) protection of cabling by conduit or cable trays. Related control: PE-2.

Control Enhancements: None.

References: NSTISSI No. 7003.

Priority and Baseline Allocation:

P1	LOW Not Selected	MOD PE-4	HIGH PE-4
----	------------------	----------	-----------

IV. Attacks on Critical Facilities?

What the Feds REALLY Worry About When It Comes To Physical Security

- Vehicle Borne Improvised Explosive Devices (VBIEDs) are generally considered to be a top government/military threat, particularly after:
 - the attack on the Marine Barracks in Beirut in 1983,
 - the Oklahoma City Murrah Building bombing in 1995, and
 - the Khobar Towers bombing in Saudi Arabia in 1996.
- If you want to better understand the VBIED issue at a visceral level, let me recommend two movies you might want to watch:
 - "The Kingdom" (2007)
 - "The Hurt Locker" (2008)

Khobar Towers, Saudi Arabia



WE Can't Worry About "Everything..."

- In the real world, we all have to “make our numbers,” and that usually means prioritizing and spending money on security measures only 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.**
- Here in Eugene, for example, we might hope that we could largely discount VBIEDs as a threat, choosing to accept that (hopefully low) risk rather than making investments in anti-VBIED technologies such as physical barriers and standoff zones, blast resistant glazing, vehicle inspection stations, specially trained and equipped bomb technicians, etc.

But Eugene Can Be a Surprising Place

- Sometimes Eugene isn't the sleepy little quiet college town we might all hope it would be.
- For example, I think most of us can remember some of the arson incidents that have disrupted the community over the past decade, including what some have referred to as the "**largest domestic terrorism case in the United States.**"
- That case, "Operation Backfire," played out (in part) right here in Eugene.

Operation Backfire



Eco-Terror Indictments 'Operation Backfire' Nets 11

01/20/06



The arson at the Vail Ski Resort in Vail, Colorado, in 1998 caused an estimated \$12 million in damages.

On 1/20, 11 people were charged with acts of domestic terrorism on behalf of the extremist Earth Liberation Front (ELF) and Animal Liberation Front (ALF) over a five-year period.

The 65-count indictment alleges the defendants committed acts of domestic terrorism between 1996 and 2001 in Oregon, Wyoming, Washington, California, and Colorado. Specifically, the indictment includes charges related to arson, conspiracy, use of destructive devices, and destruction of an energy facility.

The defendants are implicated in 17 attacks, including the \$12 million arson of the Vail Ski Resort in Vail, Colorado, in 1998 and the sabotage of a high-tension power line near Bend, Oregon, in 1999. The indictment follows a series of arrests on Dec. 7, 2005 and again earlier this month. Three suspects named in the indictment are believed to be outside the U.S.

"Terrorism is terrorism, no matter what the motive," FBI Director Robert S. Mueller said during a press conference Friday at the Department of Justice. "There's a clear difference between constitutionally protected advocacy—which is the right of all Americans—and violent criminal activity."

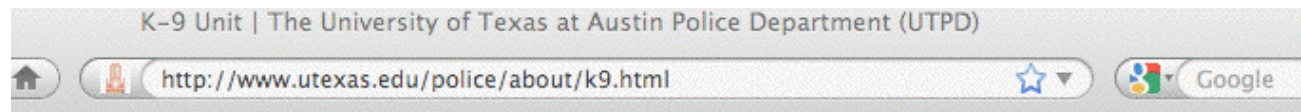
Terrorism, both international and domestic, is the FBI's top investigative priority. In this case, the FBI's Portland field office in 2004 consolidated seven independent field office investigations and dubbed it "Operation Backfire." A year-long investigation, aided by the Bureau of Alcohol, Tobacco and Firearms and other federal, state, and local law enforcement officials, yielded evidence of an ongoing conspiracy by members of ELF and ALF. On Jan. 19, the U.S. Attorney's Office in Eugene, Oregon, obtained an indictment of criminal conspiracy for the following individuals:

- Joseph Dihaas

Responding to Bomb Threats

- Terroristic threats, such as bomb threats, can also be very disruptive. There's little choice but to take them seriously until they can be investigated and ruled out.
- While many police agencies have interagency agreements allowing them to share specialized capabilities such as bomb detection dogs, a growing number of campus police departments have decided to deploy their own local K-9 units to help clear buildings in response to the bomb threats they receive.
- These dogs and their handlers should be your good friends, and routinely invited to sweep your IT facilities so the animals and their handlers become familiar with them, and the potential intricacies of their layouts, should you ever experience a real threat where time is of the essence.
- UO's DPS has recently proposed creation of a campus K-9 explosives detection unit (see <http://tinyurl.com/65ojkb9>)

University of Texas Police Department K-9 Unit



K-9 Unit

The K-9 Unit was created as a proactive measure to ensure the safety of students, faculty, staff and visitors to campus. Since September 11, 2001, UT Administrators have tried to provide for better public safety by changing procedures concerning how large gatherings are handled. The university felt that an explosive-detecting dog would be a valuable addition to the security of the campus since we are a venue for many large sporting events, concerts and other public gatherings.

The K-9 Unit enables UTPD to sweep for explosives before events begin and will help provide the public with a little more peace of mind.

Each canine and their handler completed five weeks of training at [Global Training Academy](#), a world recognized K-9 training facility in Somerset, Texas. Spike and Maatje are certified in explosive recognition and patrol.

Officer Taylor and Spike



In February 2010, UTPD welcomed Spike to the department. Officer Jason Taylor serves as Spike's handler.

Sgt. Stock and Maatje



In January 2005, UTPD welcomed its second canine, Maatje. Sgt. Robert Stock serves as Maatje's handler and joined UTPD in 2001.

University of Wisconsin Police Department K-9 Unit

//www.uwpd.wisc.edu/field-services-k9-unit.htm



Google

UWPD K-9 Unit

The University of Wisconsin Madison Police Department K-9 Unit started in May, 2002 by the efforts of K-9 Unit Coordinator Lieutenant Jason Whitney, management and the University Community. The Unit began with Czech Republic born German shepherd, Mosely. Mosely was trained in explosive detection and suspect tracking and worked with Special Events Lieutenant K-9 handler, Whitney. It is with respect that UW-Madison Police Department announced the death of Officer Mosely on March 3rd, 2010.



In October, 2003 the K-9 Unit expanded, adding a second Czech Republic born German shepherd, Rex. K-9 Rex is also trained in explosive detection and tracking and works 1st Shift Detective Bureau with his K-9 handler, Detective Shane Driscoll. Both Rex and Mosely had been trained with their handlers at Vohne Liche Kennels in Denver, Indiana. There are currently only three explosive detection K-9s in Dane county, two of them right here at UW-Madison PD.

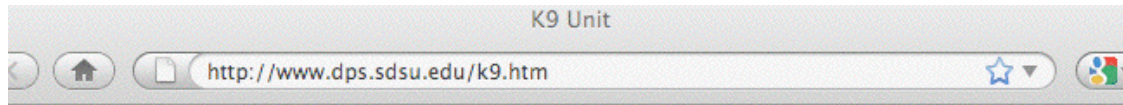
The explosive detection K-9s respond to a variety of calls for service. The K-9s respond to bomb threats, suspicious packages and tracking suspects. The explosive K-9s can most frequently be seen prior to and during Badger sporting events. The K-9s also provide dignitary protection and clearing for other special events on campus and around the state. The explosive K-9s are available upon request statewide by law enforcement agencies for explosive detection and tracking.



(1998-2006)

March 2007 brought another expansion to the Department's K-9 Unit. Born, raised and trained in Madison, WI, Casey is a Dutch Shepherd trained and certified in narcotics detection, agility and evidence recovery. K-9 Casey works 2nd shift patrol with her handler, Police Officer Cherise Caradine. K-9 Casey was trained by Madison Police Department Sergeant Christine Boyd, who coordinates and leads the Madison K-9 Unit and handled K-9 Arno

San Diego State Police Department K-9 Unit



The goal of the SDSU Police K-9 program is to enhance the effectiveness of our police officers in searching for and apprehending violent criminals, locating evidence, narcotics and explosive devices. SDSU's K-9 teams train with other agencies within San Diego County and provide K-9 support to local, state and federal law enforcement agencies.

Nemo and *Brico* also provide an important community outreach function as the K-9 teams demonstrate their professionalism to community groups throughout the year.

The SDSU Police Department is grateful to both the SDSU Aztec Parent's Foundation and the San Diego Police Foundation for funding and helping expand the size and capabilities of the police department's K-9 Unit.



Sometimes IT's Role Is Supporting Efforts to Mitigate the Impact of Severe Weather, Active Shooters, etc.

- While IT (with its high value hardware and ongoing mission critical responsibilities) is sometimes the target of attacks, other times IT's role is to support efforts to mitigate the impact of attacks.
- Since the shooting incident at Virginia Tech and passage of the Clery Act, many universities have created emergency notification programs, including things like:
 - "reverse 911" services to provide emergency information to user cell phones or email addresses, and
 - campus sirens, public address systems, electronic signage, etc.
- For more information on what some campuses are doing, see "Real Time Notification During a Disaster or Other Emergency," <http://pages.uoregon.edu/joe/notification/>
- You may also want to check out UO's emergency management site at: <http://em.uoregon.edu/>

V. Physical Security of Your Networks

Network Outages Due to Physical Network Damage

- Regardless of how skeptical we may be of other physical security threats (such as IEDs or arson risks), one **very real** threat that I think we're all willing to acknowledge is that heavy construction equipment has an uncanny ability to home in-on and accidentally cut critical buried network infrastructure.
- For the purposes of this talk, I'm going to assume that most of you DO NOT own or operate a regional or national fiber of your own. When you need wide area network connectivity, you buy what you need from a commercial network service provider.
- As a result, I'm going to omit my spiel on what you might do to directly protect your own regional or national fiber infrastructure.
- Let's talk a little about what you can accomplish via "appropriate use of purchase orders," instead.

Architecting and Building for High Availability

- One way you can improve the physical security of your wide area network is by adding additional network connectivity, thereby obtaining redundancy, excess capacity, and a degree of resiliency.
- 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!”
- One difficulty is that you may have a hard time determining the path that a given circuit or provider follows. You run the risk of purchasing "redundant" "diverse" connectivity from multiple providers that's all provisioned over the same infrastructure, thereby introducing unexpected single points of failure (ugh).
- You may need to explain your concerns and be pushy. If you're a nice guy or nice gal, your primary and backup connectivity may end up running over the same glass, and that's not good. :-)

Redundancy and Resiliency Isn't Free (Duh)

- Of course, the downside of all this is that redundancy and resiliency comes at a cost (as the saying goes, “you can get whatever level of availability you can afford”).
- The first path between two paths normally goes via the cheapest and most direct route. A diverse path (virtually by definition) will need to go via some longer/less desirable/more expensive-to-provision path.
- You also need to accept that you'll be buying capacity that you normally won't be using. (If you do rely on use of your “backup” link to have enough capacity to accommodate your normal production traffic requirement, what will you do if your primary link goes down? Your links should be able carry all the traffic at your site, so long as at least one link is still available. Alternatively you need a plan to selectively shed or de-prioritize load until you've eliminated performance-killing congestion issues.

Provisioning Multiple Links For a 100 Unit load

• Links	1 Link Lost	2 Links Lost	3 Links Lost
1 100 unit	0 units	n/a	n/a
2 100 units	100 units	0 units	n/a
3 100 units	200 units	100 units	0 units
4 100 units	300 units	200 units	100 units
2 50 units	50 units	0 units	n/a
3 50 units	100 units	50 units	0 units
4 50 units	150 units	100 units	50 units

What you should buy depends on your availability requirements, your load characteristics, and your budget. Also note that you may be hard pressed to perfectly balance your load across multiple links. Under normal (and/or emergency!) circumstances, one link might run quite hot, while another might be nearly idle.

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 an excellent 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.

But An Example of How Sometimes Having Multiple Redundant Paths Can Pay Off Big Time: Public Safety Communications On August 1st, 2007 in St Paul

The ARMER System as Implemented in the Twin City Metro Area

The ARMER backbone as implemented in the Twin Cities is composed of a large regional “umbrella” subsystem and two local subsystems that are integrated to operate as one.

The regional subsystem consisting of a number of towers throughout the nine county Twin City Metro area linked together by a redundant, dual-path microwave and fiber-optic system. (Note: The southern microwave loop of the ARMER system was inoperable on August 1 as some of the equipment was being relocated to accommodate Dakota County's transition on to the ARMER system. A second redundant pathway -- a critical fiber-optic link -- was actually carried under the collapsed bridge and was severed at the time of the collapse, but due to its alternate routing configuration, another fiber link -- a third level of redundancy -- the link destroyed in the collapse presented no communications problems.)

<http://www.srb.state.mn.us/pdf/I-35W%20Final%20Report.pdf>

[Remember, too, the triple cable outage mentioned on slide 16]

Indirect Costs

- In addition to the direct costs associated with buying diverse redundant links, you'll also potentially incur significant indirect costs.
- For example, multihoming across multiple commodity transit providers implies that you'll need a network engineer who understands BGP, border routers with the horsepower and capacity to carry a full routing table, your own ASN and your own provider independent address space, etc.
- Some organizations may decide that they just can't afford those sort of expenses (especially if a salesperson offers a great alternative offer, albeit with all your eggs in just their one basket).

Hardware Sparing

- You also want to work to ensure that if an outage does occur due to a hardware failure, you can recover from it in a timely fashion.
- For example, are you continually monitoring your network and **maintaining adequate local spares?**
- Often, particularly in smaller secondary markets, like Eugene, more expensive spares are not stocked locally, they're shipped in from regional depots in Portland or Seattle or San Francisco or Denver on an as-needed expedited basis.
- However, when multiple customers simultaneously suffer outages and all need replacement parts at the same time, or when same day courier service is disrupted due to a disaster, a lack of local spares could get ugly.
- Beware of one disaster causing other "disasters!"

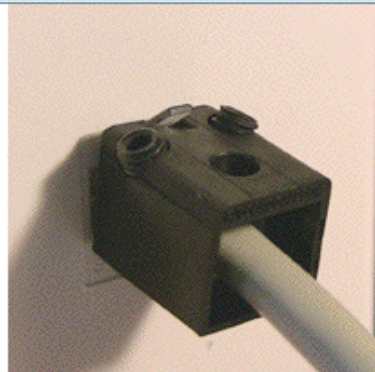
Network Confidentiality

- Most networks carry some sort of potentially sensitive information, whether that's financial information, health-related information, FERPA-protected information, or whatever.
- And if you're like most folks, you know that information sent over an unencrypted wireless like can easily be intercepted by a bad guy or gal, right? (WiFi is a broadcast medium after all)
- But do you give any thought to the possibility that your hardwire 10/100/1000-base-T ethernet connection might also be getting monitored ("sniffed")?
- Physical access to your network really simplifies the process of sniffing your/your users' traffic. Control access to wiring closets and cable runs!
- And just because a network is switched, that doesn't mean it can't be forced into flooding traffic to all ports (c.f., dsniff, Cain&Abel)

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 located 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)

The First and only Cat5 and Cat6 Jack Lock




They are sold in pairs that comes with a set of 3/32 Allen and T10 Torx set screws. Allen for low security and Torx for high security.

\$8.99 to Defeat “Secure” Fasteners...



Click on image to zoom



100 Piece Security Bit Set **drillmaster**

ITEM # 91310 MANUFACTURER: DRILL MASTER

Security bit set gives you full access to protected components

Only: ~~\$9.99~~
Sale: \$8.99

Qty: [+ Add to Cart](#)
[Add to Wishlist](#)

Availability: In stock **Shipping**

Leaves the warehouse in 1-2 business days. Economy Ground & Express Shipping available.
(Exclusions may apply)

Customer Rating: ★★★★★ 11 Review(s) | [Add Your Review](#)

Description of Drill Master 91310

This 100-piece set includes security bits that let you work with hex, hollow hex, Pozzi, Torx, hollow-tip Torx, square and spline fasteners.

- Includes slotted and Phillips bits
- 1/4" hex shaft
- Rugged chrome vanadium construction
- Blow-molded case with individual compartments

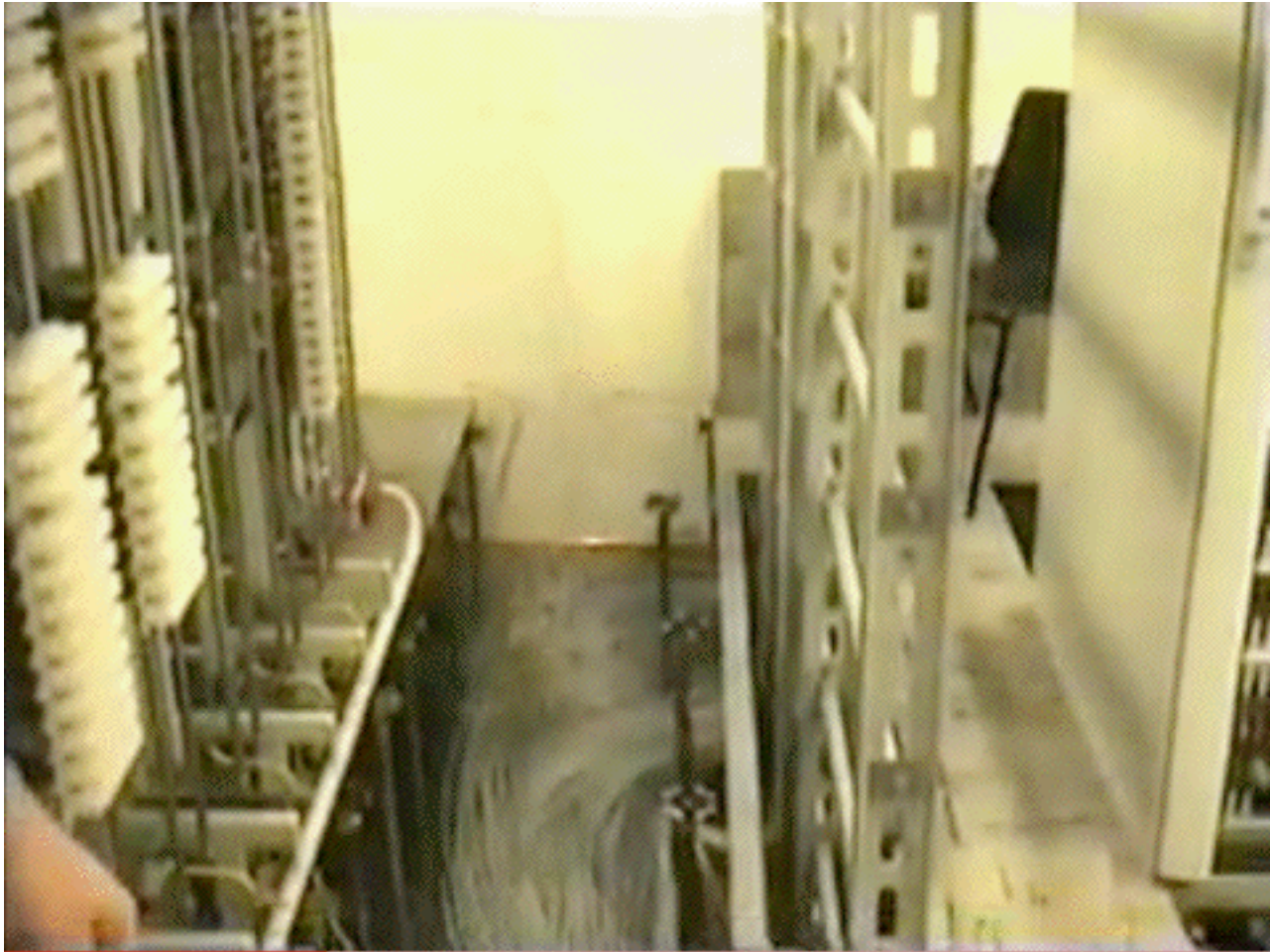
Hex end to 1/4" drive adapter, magnetic hex bit driver, hook hanging bit (Y- design), 1/4" hex to 1/4" socket drive bit and 1/4" hex wobble adapter -also includes 8 Phillips, 8 Pozzi drive, 9 slotted, 4 spanner, 9 torque, 4 tri-wing, 9 hollow tip torque, 3 torque-set, 9 metric hex, 4 square, 10 SAE hex, 3 spline, 6 hollow metric hex, 6 hollow SAE hex and 3 clutch bits

VI. Physical Security of Your Facilities

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 such as key network equipment (optronics, routers, switches, etc.), as well as servers, critical staff, documentation, media, etc.
- Those facilities also need to be physically secure.
- Physical security can mean, among other things, that the facilities aren't likely to be damaged by a deluge or other natural disaster.

A Flooded Data Center...



Video: http://www.youtube.com/watch?v=ANU-oSE5_hU

Time: 2:01

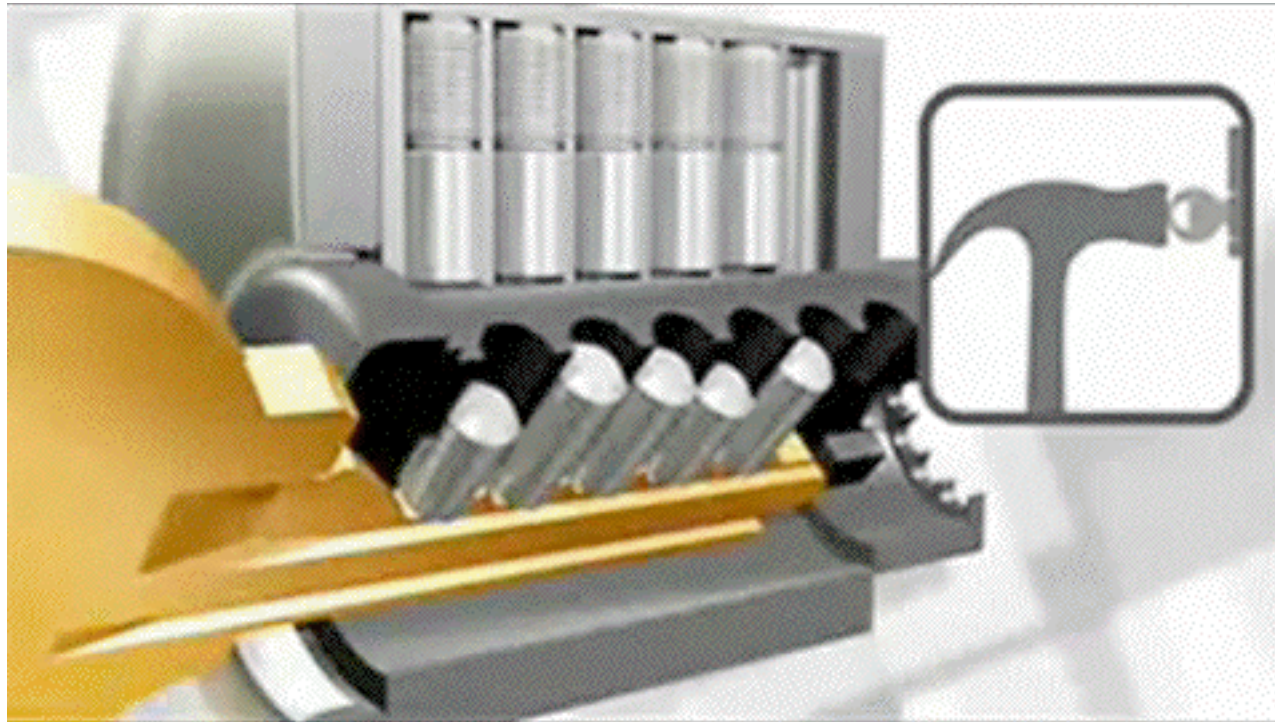
Locks

- Once we get beyond things like protecting a site from flooding or other natural disasters, physical security often focuses on 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," but because locks are used so many places related to computing and networking, let's talk a little about locks.

Surreptitious Opening of Traditional Pin Tumbler Locks

- Even though traditional pin tumbler locks, such as the locks used on most doors, have well known limitations, they still form at least part of the physical security at most sites, including many computer or networking sites.
- If you think that traditional pin tumbler locks provide anything even *remotely* approaching reasonable security, I'd urge you to think again.
- In particular, you should learn about “bump keys.”

Video: How Lock Bumping Works



Video: <http://www.youtube.com/watch?v=7xkkS2p7SuQ>

Time: 2:04

If Detection Isn't A Problem...

- 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 exposed outward-swinging external door hinges, too!

Hinges

[://www.statefarm.com/learning/be_safe/home/burglary/learning_besafe_atm_burg_hing.asp](http://www.statefarm.com/learning/be_safe/home/burglary/learning_besafe_atm_burg_hing.asp)

Door Hinges and Home Security

Door Hinges on Exterior Swinging Doors

Although most people don't give a second thought to the security options available in door hinges, there are door hinges available that can provide better security.

In some parts of the country, it is common to see doors swing out. When the door swings outward, the hinge pins are typically exposed on the outside of the house.

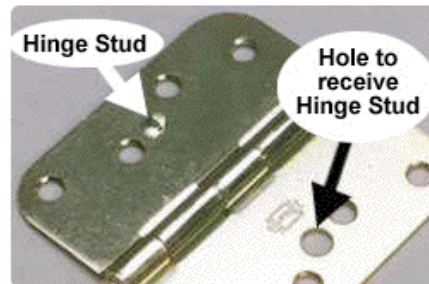
This could allow an intruder to tap the hinge pins up and out, and lift the door off its hinges, removing the door without unlocking it.

There are several door hinge designs available that make it more difficult to remove the hinge pins.



Non-Removable Pins

On these hinges, the pins are held in place by a setscrew. If the door is in the open position, the setscrew is exposed and can be retracted, and the hinge pins removed. If the door is closed, the setscrew cannot be accessed.

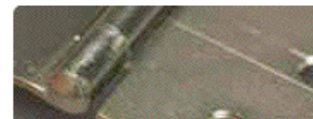


Safety Studs

These hinges come in full mortised type only, meaning the hinge sits in routed-out insets in the door and frame. Studs extend from one hinge leaf and a hole is punched in the corresponding position on the opposite leaf. When the door is closed, the stud sits in the hole. If the hinge pin is removed, the door still cannot be taken off its hinges because the stud holds it in place.

Fast-Riveted (Crimped) Pins

These hinges are designed so the hinge pin cannot be removed. The hinge pin is made longer than the hinge height, inserted into the hinge, and spun on the end to create a rivet-type end on the top and bottom of the pin.



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 gas 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
- The ultimate? The Navy has approved the S&G 951 High Security Padlock, but at >\$1,000/lock, it might be, um, a little pricey



A S&G 951 Padlock

DoD LOCK PROGRAM

http://www.dscp.dla.mil/gi/locks/

Google

High Security Padlocks



- 5340-01-217-5068: S&G 951, Padlock, Key Operated. High Security Shrouded Shackle
*For use by DoD personnel and active duty U.S. military **ONLY**.*
- 5340-01-449-4346: S&G 951, Padlock, Key Operated. High Security, Shrouded Shackle (with R1 key-way)
For use by all other Federal agencies and DoD contractors.

(Different key-ways are intended for use by different audiences)

Keys

- Key-related issues are another reason why traditional locks often provide mediocre security.
- In many environments, 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 which all use 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

Part of A Keys Control Checklist from the USDA

KEY CONTROL

1. Is a key-control system in effect? _____

2. Who is responsible for the key control system?

Name:

Phone#:

Email Address:

3. Are building entrance keys issued on a limited basis? _____

16

C:/USDA Checklists/USDA Physical Security Checklist

USDA Physical Security Inspection Checklist

DRAFT

YES NO

4. Are master keys kept securely locked and issued on a strictly controlled basis?

5. Can the key-control officer replace locks and keys at his discretion?

See: <http://www.usda.gov/da/physicalsecurity/physicalcheck.pdf>

Alternatives to Locks and Keys

- Many facilities have moved to “key cards” (swipe cards, prox cards, etc.) as an alternative to traditional locks & keys
- Key cards offer distinct advantages over traditional locks and 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.
- Sometimes, though, key cards may offer only an illusion of security. For example, some may be easily brute forced using widely available tools.

Some Prox Cards Tools

- Some resources are mentioned in <http://www.mcafee.com/us/resources/white-papers/foundstone/wp-proxbrute.pdf>

-- Proxmark III: <http://www.proxmark3.com>

-- Proxpick: <http://www.proxpick.com/>

-- ProxClone: http://proxclone.com/reader_cloner.html

- Also worth a read:

“The RFID Hacking Underground,” Wired, May 2006

<http://www.wired.com/wired/archive/14.05/rfid.htm>

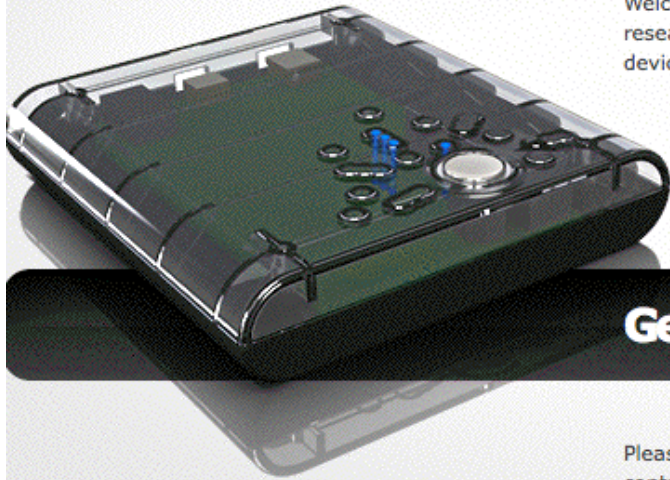
and

<http://rfidiot.org/>

Proxmark3



Welcome to the Proxmark III online store. We offer the fastest way to get started researching RFID and Near Field Communication systems using the powerful Proxmark III device.



- Pre-programmed thoroughly tested boards
- Read & emulate any RFID tag
- Orders ship within 2 business days

Get Yours Today!

Please see the **FAQ** and **Terms of Sale**. Additional information can be obtained by contacting sales@proxmark3.com. This website requires that javascript be enabled to function correctly.

Enclosed Proxmark III	\$399	Add to Cart
Naked Proxmark III - SOLD OUT	\$229	Add to Cart
Low Frequency Antenna	\$59	Add to Cart
High Frequency Antenna	\$59	Add to Cart
Tag Bundle	\$12	Add to Cart

FWIW, Many Swipe-Style Cards Aren't Perfect Either



July 17, 2008

After Security Breach, Harvard Unveils New IDs

Encryption technology in new proximity ID Cards to strengthen security in FAS Buildings

By [Abby D. Phillip](#), CRIMSON STAFF WRITER

The Faculty of Arts and Sciences (FAS) announced last week that students, faculty, and staff will receive new identification cards that use contactless Smartcard technology when they return to campus this fall.

The upgrade comes less than a year after Theodore R. Pak '09 was caught creating duplicates of the Harvard University ID (HUID) cards belonging to University President Drew G. Faust, Assistant Dean of the College Paul J. McLoughlin II, and Dunster House Superintendent H. Joseph O'Connor.

Pak's hack revealed a significant security flaw in the more than 15-year-old swipe card system, as he was able to gain access to buildings and gates across campus with only knowledge of HUID numbers and a \$200 card reader bought from eBay.

Assistant Dean for Physical Resources Michael N. Lichten said that the Pak incident "was a motivator for us to move more quickly in putting the new system in place."

Prior to the Pak incident, HUID numbers were available to a number of individuals at the University including undergraduate User Assistants, Harvard University Dining Services workers, building managers, and freshman proctors. The University has since strictly restricted the access to these numbers, putting in place a number of protocols that limit how and when they can be displayed and accessed by members of the Harvard community.

The new cards are intended to bolster the security of FAS buildings by adding crucial encryption technology and more complex security procedures.

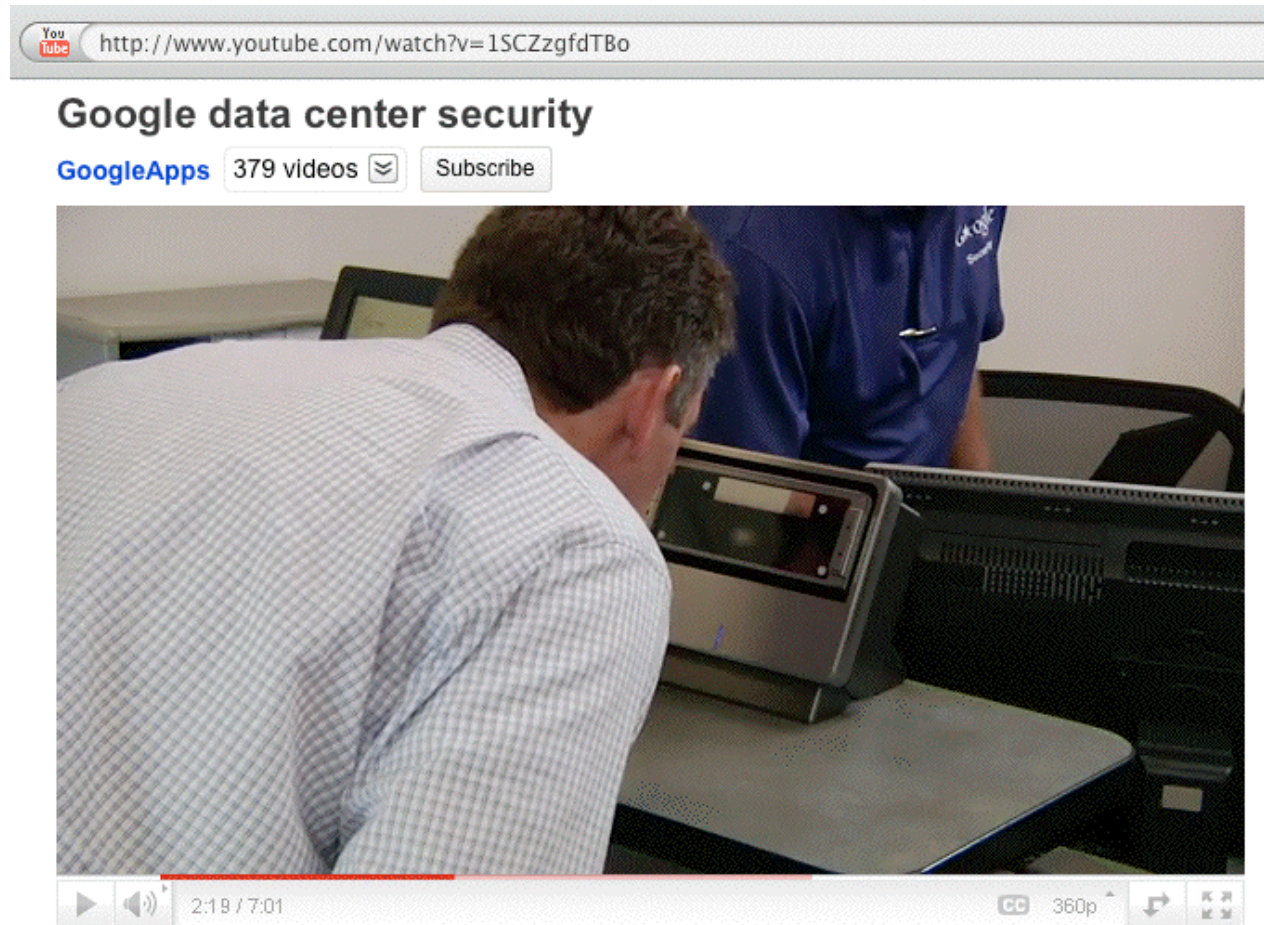
Lichten said that unlike the previous card system, which functioned directly on unencrypted HUID numbers, the new proximity cards will carry encrypted information that must match data saved by the security system on who is given access to each building.

Biometrics

- Biometric systems use your physical characteristics to decide if you should or shouldn't be granted access to a facility or resource.
- Examples include:
 - fingerprint or hand geometry readers
 - iris and retina scanners
 - voice identification
 - facial recognition
 - signature recognition
- Nice discussion of biometric issues in GAO-03-1137T, "Challenges in Using Biometrics," <http://www.gao.gov/new.items/d031137t.pdf>
- I'm not a huge fan of biometric solutions, but that's just me.



Example of One Site That Is Using Biometrics



Video URL: <http://www.youtube.com/watch?v=1SCZzgfdTBo>

Building Security:

Piggy Backing/Tailgating/Social Engineering

- 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, or by manipulating basic social courtesies.
- A nice example of manipulating basic social courtesies, mentioned to me by a colleague recently: approach the door to a controlled area carrying what's obviously a heavy box. It takes a pretty "heartless" person to not help by holding the door. Social engineering is just as big a problem for IT physical security, as it is for phishing attacks.
- An attendant at the door can also ensure that everyone coming in "cards in" as may be required (but I know that this is something that many higher education sites have trouble enforcing).
- Floor to ceiling turnstiles or mantraps (interlocking pairs of doors) can be used to help physically prevent these sort of phenomena.⁷³



Single Entry Interlocking Door System

The TAP-100 Interlocking Door System is a fully programmable cylindrical portal which can be designed with metal detection, armored glass, and uni-directional or independent bi-directional electrical controls. The system can be integrated with any type of access control system.

Characteristics

- Prevents piggybacking
- Small 32-1/4" diameter cylindrical portal
- Integrates with any access control system
- Optional bullet resistant glass
- Optional metal detection
- TAP-100EE: Integrated with emergency exit to allow automatic opening of curved doors and swing door simultaneously

Building Security: Stay Behinds

- 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.
- For example, a stay behind visitor can open an unalarmed external door from the inside, thereby allowing entry of additional people.
- Finding stay-behinds is easier if a building has motion sensor alarms deployed, or if the organization routinely uses security dogs to sweep sensitive buildings at closing time. Routinely lock all places where an unauthorized person might hide, out of sight, until the building empties (such as supply closets, unused offices, etc.)

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

- Sometimes you'll see a high security lock "protecting" a room with a hollow core door, 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 just punch through the door or sheet rock walls, or climb in above the suspended ceiling or below the raised floor. (Embedded heavy gauge wire mesh can at least make that sort of through-the-wall or through-the-ceiling or floor entry a little more difficult)
- Similarly, have you secured your roof? Or could someone use an extension 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).

Windows (The Glass Type, Not The Microsoft Type!)

- Windows represent another potentially important physical security vulnerability.
- We all love fresh air and nice views, but some windows are large enough to allow a skinny thief equipped with a rock to break in.
- Other times, windows might be left ajar and unattended, so that an intruder doesn't even need to break anything to gain access – they may just be able to reach in, or crawl in.
- **Important:** your ability to secure windows with security grills or bars may be limited by building code requirements and life safety concerns in case of fires or other emergency. Be sure that any mechanisms you deploy to secure window issues DO NOT create life safety hazards.
- While you're working on improving your window security, you may also want to consider deploying reflective film. Reflective window film may reduce the ability of casual pedestrian traffic to "window shop" for valuables, and may also help reduce unauthorized viewing of what's on employee LCD panels (see also 3M's line of display privacy filters).

Fencing

- University campuses aren't like industrial or government facilities, but if you can add a fenced perimeter around critical facilities, that fence will immediately add significantly to your site's physical security.
- Government and military folks (who worry about things like VBIEDs, as discussed earlier) like a wire cable-reinforced perimeter fence that's ideally at least fifty feet away from the facility that's to be protected, built from 9 gauge (or heavier) chain link, seven feet or more 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.
- That may all be a bit much for university environments, but if you can deploy it, it's another layer of physical security.

Exclusion Zones, Intrusion Detection & Landscaping

- Most fences (particular with proper signage) 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.
- Any landscaping should not provide hiding spots for intruders.
- Any trees near or overhanging a security fence should also be trimmed or removed to prevent the tree from being used as a pathway over the fence.

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 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 security guards and local 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 all critical facilities.
- 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.

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 concerns.
- 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 Halon alternatives: <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.

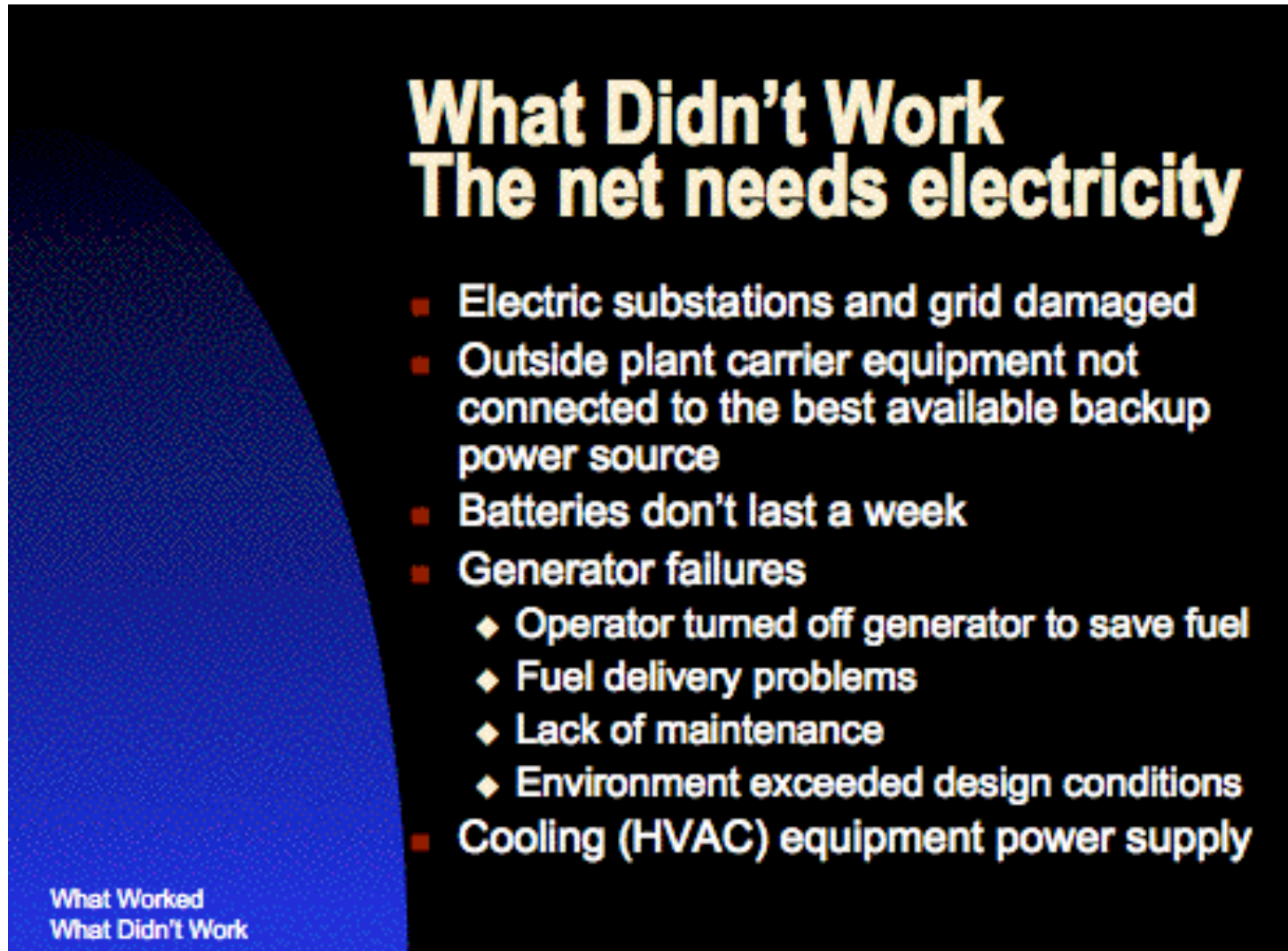


Source: <http://tinyurl.com/65mrh3w>

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.

An Example from 9/11



What Didn't Work

The net needs electricity

- Electric substations and grid damaged
- Outside plant carrier equipment not connected to the best available backup power source
- Batteries don't last a week
- Generator failures
 - ◆ Operator turned off generator to save fuel
 - ◆ Fuel delivery problems
 - ◆ Lack of maintenance
 - ◆ Environment exceeded design conditions
- Cooling (HVAC) equipment power supply

What Worked
What Didn't Work

<http://www.nanog.org/meetings/nanog23/presentations/donelan.ppt>

VII. Personnel

Protecting Your Personnel (And Their Families)

- Just as you protect your personally identifiable information, networks, systems, and facilities, you should also protect what's ultimately your most valuable asset: your staff (and potentially their family members).
- Why worry about staff family members? Consider incidents such as the recent kidnapping of anti-virus expert Eugene Kaspersky's 20-year-old son Ivan* -- that incident caused a lot of concern for many security experts. Fortunately, the incident worked out okay for the Kaspersky family in the end, but it could have been a tragic event.
- If you cannot effectively protect all critical staff and their families, you may want to consider "key person" insurance to hedge your business against the effects of their potential loss.

* "Russian Investigators Free Kaspersky's Son, No Ransom Paid,"
<http://www.pcmag.com/article2/0,2817,2384235,00.asp>

A Few Potential Personnel Protective Measures

- Limit the information about employees and their work (particularly any work on sensitive projects) that may be available on company web sites, in newsletters, and in brochures, etc.
- Employee directories should receive particularly careful review to make sure that personal information (such as employee home addresses) doesn't get disclosed.
- Limit facility access by the public. Tours and other visits, for example, are a great opportunity for bad people to check out your physical security measures, looking for any weaknesses.
- Provide secure parking. Employees may be targeted for attack while walking to or from their vehicle, or their vehicle may be burglarized or tampered with if left in an insecure location.
- Provide a means by which employees can report suspicious activity, whether that's an outsider reconnoitering your offices, or a co-worker who's making threatening comments.

Personnel Can Also Be A Potential Risk

- 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 – they're literally "insiders."
- Historically many IT sites 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 infrastructure.
- Don't neglect personnel background checks in your eagerness to fill hard-to-fill positions!
- Be sure to discuss any planned background checks with your Legal Counsel and Human Resources Department, since specific notice and consent requirements or other limitations may apply, and vary from state to state.
- You may also want to schedule periodic re-reviews to see what, if anything, may have changed.

ID Badges

- ID badges are another routine component of personnel security programs, and become necessary when an organization grows beyond a size where “everyone knows everyone” and “everyone knows what everyone should (or shouldn’t) be doing.”
- Ideally, ID badges would:
 - identify the person bearing the badge (“Sam Anderson”), and make it easy for third parties to verify that the right person has that badge (e.g., the picture on the badge matches its user)
 - give the person’s status (“employee”, “visitor”, etc.) and role (“senior network engineer”, “custodian”, etc.)
 - signal any atypical access (“machine room access allowed” or “must be accompanied at all times”)
 - include a magstripe or barcode that allows the credential to be easily verified against an authoritative database
 - be difficult to forge, resistant to unauthorized modifications, hard to accidentally damage, and cheap

Credentials and A False Sense of Security

- While ID badges have the potential to improve security if properly used, sites need to be on guard against letting ID badges lull them into a false sense of security. Just because someone has an ID badge doesn't mean that they should be immune from being challenged if they're somewhere they shouldn't be, or doing something they shouldn't be doing.
- Credentials should also be challenged and verified if the person presenting them isn't known, or just "feels wrong" (trust your paranoia).
- For example, it has been reported that penetration testers have been routinely able to gain unauthorized access to sterile areas of airports and sensitive federal facilities by displaying bogus law enforcement credentials. Such access is particularly troubling when those individuals are allowed access with firearms or other weapons.

An Example of Credential Abuse From the GAO

“Our undercover agents were 100 percent successful in penetrating 19 federal sites and 2 commercial airports. We were able to enter 18 of the 21 sites on the first attempt. The remaining 3 required a second visit before we were able to penetrate the sites.

At no time during the undercover visits were our agents’ bogus credentials or badges challenged by anyone. At the 21 sites that our undercover agents successfully penetrated, they could have carried in weapons, listening devices, explosives, chemical/biological agents, devices, and/or other such items/materials.

At each visit, our agents carried bogus badges and identification, declared themselves as armed law enforcement officers, and gained entry by avoiding screening. At least one agent always carried a valise.

Sixteen of the sites we visited contained the offices of cabinet secretaries or agency heads. At 15 of these sites, our undercover agents were able to stand immediately outside the suites of the cabinet secretary or agency head. In the 5 instances in which our agents attempted entry into such suites, they were successful. At 15 of the sites, our agents entered a rest room in the vicinity of these offices and could have left a valise containing weapons, explosives, and/or other such items/materials without being detected. Except for one agency, we made no attempt to determine whether any of the cabinet secretaries or agency heads were present at the time we visited their agencies.

At a federal courthouse, our agents were waved through a magnetometer but not screened. A briefcase that one of the agents carried was not checked. The agents were escorted to a gun box room, which they were permitted to enter alone. They were then instructed to lock their weapons, but no one supervised or observed the actual surrender of the agents’ weapons.

At the two airports we visited, our agents used tickets that had been issued in their undercover names for commercial flights. These agents declared themselves as armed law enforcement officers, displayed their spurious badges and identification, and were issued “law enforcement” boarding passes by the airline representative at the ticket counter. Our agents then presented themselves at the security checkpoints and were waved around the magnetometers. Neither the agents nor their valises were screened.”

Source: GAO/T-OSI-00-10, “Security Breaches at Federal Agencies and Airports,” May 25th, 2000, <http://ntl.bts.gov/lib/11000/11400/11410/os00010t.pdf>

VIII. "Information Leakage"

“Information Leakage” (FISMA PE-19)

- The final area of physical security we might consider is what FISMA PE-19 calls “information leakage.”
- If we weren't talking about physical security today, when you hear the term “information leakage,” the first thoughts that would probably come to mind would probably include:
 - sniffing unencrypted network traffic
 - SQL injection attacks (potentially extracting PII or other confidential data in unanticipated ways)
 - malware (such as “banking trojans”) eavesdropping on user financial data
 - BGP route injection attacks (“BGP shunts”)
 - DNS poisoning
 - etc.


Physical Surveillance Of Your Personnel

- The physical analog to some of those network-based eavesdropping attacks would be physical surveillance of personnel using what's colloquially known as “bugs.”
- For some reason, while most people are all too willing to believe that hackers and malicious software exist and could spy on your online activity, they are often skeptical that there are physical surveillance devices that are an equal or greater threat.
- Put another way, some people think that **“physical surveillance devices are something that only the tin foil hat crowd tends to worry about. No one’s going to bother ‘bugging’ my computer or my office or my car.”**
- I’m happy that those folks are feeling so physically secure, but that sense of security may be unwarranted.
- Physical surveillance devices DO exist and do get used.

Simple Example: A Hardware Keylogger

http://www.keycobra.com/wifi-keylogger.html

New KeyDemon Wi-Fi Premium Keylogger ^{new}



KeyDemon USB & PS2 Wifi Hardware Keyloggers just released!

These **wireless wifi keylogger** is packed with state-of-the-art electronics: **two powerful processors**, a full **TCP/IP** stack, a **WLAN** transceiver, and **2 Gigabytes** of memory.

Besides standard [PS/2](#) and [USB keylogger](#) functionality, it features remote access over the Internet. This wireless keylogger will connect to a local **Wi-Fi Access Point**, and send **E-mails containing recorded keystroke data**. You can also connect to the keylogger at any time over TCP/IP and view the captured log. All this is a device less than 2 inches (5 cm) long!


How the Wifi Keylogger work?

The main principle is very simple though: **just plug the keylogger in-between the keyboard and computer.**

The KeyDemon Wi-Fi Premium Keylogger incorporates a built-in WLAN transceiver and TCP/IP stack, meaning it can connect to the Internet through a Wi-Fi Access Point. To do that, you must provide it some basic data, such as the Network ID and password (just like any WLAN device).

Once connected to an Access Point, the keylogger will start sending E-mail reports with captured keystroke data to any recipient E-mail address you supply. This means you can keep track of what's happening on the monitored computer from any place throughout the world, just by checking your mailbox!

New WiFi Keylogger




USB Version
Now Only \$179.95!
(limited time only)

[Buy Now](#)

30 Day Money Back
Guarantee!

Invisible Keylogger Pro
Software included FREE!



More Hardware Logging Gear

<http://www.keelog.com/> Google

KeyDemon Wi-Fi Premium



The world's first hardware keylogger with **built-in Wireless LAN** support! This keylogger connects to the Internet through an Access Point, and sends **captured keyboard data as E-mails**. With this **Wi-Fi hardware keylogger**, you can silently monitor a computer from anywhere in the world, just by checking your mailbox! Ultra stealthy, undetectable for software. [\[more...\]](#)

NEW

ver. **USB 2 GB** - \$149.00 | €104.00
ver. **PS/2 2 GB** - \$139.00 | €97.00

VideoGhost DVI / HDMI / VGA

NEW Want to take key-logging to the next level? Grab entire screenshots with this **hardware video logger**! This **tiny framegrabber** hooks up to the **DVI, VGA, or HDMI** port of the graphics card, and silently records a **screenshot every few seconds**. You can later view all captured frames as **JPEGs**, by switching this video-recorder to a **2 Gigabyte USB flash drive**. Patent pending, edge cutting technology at an affordable price! [\[more...\]](#)



ver. **DVI 2 GB** - \$169.00 | €118.00
ver. **HDMI 2 GB** - \$169.00 | €118.00
ver. **VGA 2 GB** - \$169.00 | €118.00

Eavesdropping

- Just as your computer may have a hardware “bug” attached to it, so, too, in some circumstances your data center or offices may be end up with a physical bug (surreptitious microphone or camera).
- While popular television shows frequently show these devices being easily detected, in reality, at least when professional quality equipment is used and installed by a skilled professional, it can be difficult to detect and neutralize those bugs (the process of locating and defeating bugs is normally referred to as “technical surveillance counter measures” or TSCM).
- If you remain skeptical that bugs are an real physical security issue, or that they can be difficult to detect and remove, I recommend you review the presentation: “Phone Talk,” http://www.tscm.com/Phone_Lecture_2009/Phone_Lecture_Reston_VA-2009.htm (167 slides)

(Un)Trustworthy Hardware?

- “Information leakage” and “physical security problems” take on a profound new meaning if you can potentially end up with counterfeit hardware, or hardware made with counterfeit chips.
- I would encourage everyone to become familiar with the threat I’m referring to in this area – a nice briefing is the FBI PowerPoint deck entitled, “FBI Criminal Investigation – Cisco Routers,” as embedded in graphical form in “FBI Fears Chinese Hackers Have Back Door Into US Government and Military,” see <http://www.abovetopsecret.com/forum/thread350381/pg1>
- See also the excellent article “Dangerous Fakes,” http://www.businessweek.com/magazine/content/08_41/b4103034193886.htm
- Buying counterfeit products is one physical security risk, but other physical security risks are associated with disposing of surplus/no longer needed hardware on the other end of the cycle...

Dumpster Diving and Surplus Equipment

- Historically, many crackers got their start by digging interesting computer and networking gear out of corporate dumpsters (a fine art known as “dumpster diving”).
- 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, even if the system itself no longer boots/runs.
- Beware of amateur efforts at rendering hard drives unusable – staff members can easily hurt themselves while attempting to destroy surplus equipment with sledge hammers or other improvised tools (one particularly dangerous example involved amateur use of thermite!). Surprisingly, information may still be able to be recovered from an apparently “destroyed” drive.
- Consider hiring a contractor to crush or shred your drives, or (if your volume is large), perhaps get your own crusher/shredder.



Model 0300 Low/Medium Volume Hard Drive Shredder

DESTROYS HARD DRIVES, OPTICAL MEDIA AND ASSORTED ELECTRONIC DEVICES

When it comes to the fast, safe, easy destruction of hard drives, nothing outperforms the Jackhammer™ Hard Drive Shredder from SEM.

Small footprint unit designed for low volume shredding, up to 500 laptop style drives per hour and 200 standard desktop style drives per hour. Single phase 120V power makes it ideal for office environment use. Designed with Operator Ease-of-use and safety in mind, **system features include:**

- Mailbox style feed opening
- Electrical limit switches to shut down machine when accessing cutting system or waste removal
- Easy access waste collection bin
- Integrated HEPA Filter
- Auto shut down when collection bin is full
- Illuminated controls to provide operator awareness of system status.
- Heavy duty casters for easy mobility



[see larger picture](#)

Model 0300 Jackhammer Low/Medium Volume

MSRP:
\$29,609.00

- ☒ Online Commercial:
\$21,250.00
- ☐ GSA Contract:
\$18,950.00

1 Buy Now

More Information

[View Datasheet \(PDF\)](#)
[View Complete Catalog \(PDF\)](#)
[View Video](#)

What About Software Drive Sanitization?

- If you don't have access to hardware drive destructors, or a drive destructor service, assuming the disk is still operable, another alternative is software drive sanitization. While this is less assured than hardware disk destruction, it is at least a little better than nothing.
- A couple of starting points:
 - Darik's Boot and Nuke (DBAN): <http://www.dban.org/>
 - Apple's discussion of erasing disks securely (OS X 10.4 or later): <http://docs.info.apple.com/article.html?path=DiskUtility/10.5/en/duh1011.html>

Confidential Documents and Removable Media

- Sensitive ***documents*** and ***removable physical media*** also need to be shredded, incinerated, or otherwise securely destroyed.
- Note that not all shredders are equally effective (e.g., wide strip shredders are not as good as cross cut micro confetti shredders).
- Shredders also **must be used properly** (simple example of a user error compounding a poor technology choice: by feeding documents into a strip shredder sideways, you might end up with strips that have whole sentences intact!)
- You should also be aware that document reconstruction software now exists that automates the jigsaw-puzzle-solving-like process of "unshredding" shredded documents.
- Lastly, for those who outsource their document destruction, be sure you properly secure any mobile containers you use to accumulate sensitive documents meant for eventual pickup!

IX. Conclusion

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 an hour, 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 begin working on this important area.
- Hopefully this talk will at least provide some starting points for that conversation.

Thanks for the Chance to Talk This Evening!

- Are there any questions?

- Contact me:

Joe St Sauver, Ph.D.

joe@uoregon.edu or joe@internet2.edu

541-346-1720

- Copies of these slides are available online at

<http://pages.uoregon.edu/joe/eugene-it-pro-forum/>