

# IT Risk Assessment and Remediations

## CLAS Statistics

September, 2007

### **1 Local choices of mitigations to likely problems**

The department has a vanilla style of system administration, as recommended and described in industry-standard books like the *UNIX System Administration Handbook* by Evi Nemeth, Garth Snyder, and Trent R. Hein. That material won't be repeated here; instead, this document describes the local choices made within that framework and the culture of the typical university style of system administration.

### **2 Risk: A bus runs over the sysadmin**

When the existing sysadmin is lost due to accident or job change, how long is it before the previous level of service is restored? How long before the system has a serious failure merely because it is left unattended? What ordinary operations include a manual component supplied by the sysadmin, such as tape changes? How long before a new sysadmin can do routine modifications, such as account creations and deletions?

#### **2.1 Remediation**

The machines are deliberately maintained in a vanilla style, so that existing documentation from upstream sources will match what the replacement sysadmin will find. The backups are held in the CNS TSM system, which is widely understood on campus. A couple faculty members understand the big picture of the site, provide system administrative continuity and institutional memory, and are able to dig up the details themselves if they need to.

### **3 Risk: Viruses and trojans**

Viruses, Trojan horses, Spam, Spyware, Phishing, Script kiddies, ID theft, and credit card theft have become a single, blended, synergetic threat. Malware has now become an organized criminal enterprise, done to professional programming standards. Please see the references in this section for a much more detailed discussion.

### 3.1 Windows

Defendable estimates for the time a fully-protected Windows machine is connected to the network to its takeover range from minutes to a month. My personal experience of all Windows users I know suggests no longer than a month.

Most awareness of Windows viruses comes from user reporting of mis-operation. However, since the creation of Windows viruses has gained the efficiencies of open source, and frameworks are freely available into which black hats need only drop in a payload, I believe there must be many viruses which penetrate department machines successfully and remain undetected. I believe that it is mostly the poorly-programmed viruses, or wars between rival gangs of virus controllers, which come to our attention. Man-power limits to the frequency of reloading machines suggest that most Windows machines are cracked most of the time, and there exists a continual chain of remote access through Windows. Users find the need for complete MS Office compatibility sufficiently necessary for academic collaboration that the losses from the associated viruses are tolerated.

### 3.2 Linux

As the reliability of Linux is so much higher than Windows, anomalous operation stands out more clearly as an unusual event. Through the combination of greater quality of security features plus cultural factors, the risk of Linux to viruses and trojans is much lower.

### 3.3 Remediation

Windows has the recommended collection of antivirus, automatic updates, IE security zones and so forth turned on. It's the best setup available short of filtering their network access so much it amounts to unplugging them, which would render them worthless.

Except for a few legacies, user-maintained laptops are now given connections only through the CNS UFW wireless, which has a variety of scanning and network monitoring features to identify attacks in progress and disable that connection. This has drastically reduced our reports of attacks mounted from laptops brought in from the outside.

Incoming email is scanned for viruses and executable file extensions, and positive results are diverted to separate spam and virus folders. The recommended email client, Thunderbird, contains additional personally-trainable filtering which is recommended for use. Greylisting rejects the bulk of our spam, which often contains viruses.

See also:

- Section: "Risk: Remote breakin to individual machines"
- <http://www.cs.auckland.ac.nz/~pgut001/pubs/blended.pdf>
- [http://www.cs.auckland.ac.nz/~pgut001/pubs/malware\\_biz.pdf](http://www.cs.auckland.ac.nz/~pgut001/pubs/malware_biz.pdf)

## **4 Risk: Remote breakin to individual machines**

### **4.1 Linux**

Linux log files show thousands of attempts to guess usernames and passwords per machine per week. Other attacks are believed to exist, but they are rejected without logging errors because no software is running which listens to those attacks.

### **4.2 Windows**

Windows does not offer robust logs, and the evidence of a successful breakin tends to be concealed by the breakin, so attack frequency is hard to determine. Some data is available from CNS sniffing the network for common virus control channels such as IRC. The attack rate is believed high due to the high effectiveness of such attacks and the general quantity of virus problems.

### **4.3 Remediation**

Windows has the recommended collection of antivirus, automatic updates, IE security zones and so forth turned on, but the nature of these is by necessity reactionary and they miss most novel threats. No technical means to audit changes to Windows is available that is also practical, affordable, and fits into university-style operations. When breakin damage accumulates sufficiently that the user has a sustained total work stoppage, or the machine is detected attacking another, the machine is wiped and reloaded.

Technical means are in place to audit Linux machines on a per-file basis. Proving there is no filesystem damage, however caused, is a not-uncommon step in the debugging of misbehaving software or hardware. There is the expectation that security-related problems can be debugged and eliminated.

## **5 Risk: Systemic remote breakin that overwhelms**

The scenario is that enough of the department is under sufficient remote control, and the actions the remote controller is taking are damaging enough, that turning all of the affected machines off until the situation is brought under control seems like a reasonable choice. I believe that, like hurricanes, it is only a matter of time before this happens to us, and we should organizationally expect to have to clean up after a computer virus “storm” every few years.

### **5.1 Remediation**

Given a calm and reasoned response, the biggest negative consequence is probably the lost time and work disruption. We should not lose professional credibility from being successfully attacked, instead we can retain it by cleaning up and restoring function in a straightforward and professional manner.

Tell the TSM administrator to put a freeze on our site so existing good data can't be displaced by bad data in incoming backup streams. Tell the rest of campus what's going on, so they don't think we're intentionally attacking them or acting flaky. Invite the TSM administrator to contribute to our recovery plans; the TSM admin has substantial flexibility to prefetch caches so as to make restores go much faster than they ordinarily would. We are a small site, and we can comfortably fit entirely in their cache.

Remain open to research from the net for medicine to stop further breakins. The Morris worm revealed that sites that stayed connected and accepted damage while researching did a lot better than sites that disconnected. Firefighting will not work in this situation. Put efforts into finding a fix, rather than reloading things the same way just be broken into again.

If it seems simplest, roll back to before the attack, throwing away a day or two's work. Restore from good data, and get the medicine in place before exposing to reinfection.

## **6 Risk: Direct strike by hurricane or pressure washer**

In some rooms in Griffin-Floyd, especially on the North end, the joint between the window sashes leaks or sprays water that is vigorously blown at it.

In a hurricane the power may go out or gyrate, and computers are not unlikely to be damaged by this experience. Servers in the closet are on UPSes, whose batteries are of reasonable age, but desktops are not.

### **6.1 Remediation**

Expect the windowsills to get wet. Move things off the windowsills and cover the near end of the desk with plastic.

Power off the desktops in anticipation of power spikes and surges. Turning desktops off will also reduce heat and humidity stress on them if the air conditioning fails, and permits covering them up with plastic to protect from window leaks.

Leave the server closet running to maintain the department's electronic presence and allow working from home, unless sustained AC or power loss seems likely.

## **7 Risk: Air conditioning failure in the server closet**

Every few months physical plant breaks the air conditioning in the server closet with a software upgrade on the building controller. I believe this is driven by a game of hot potato about which buildings will conserve energy. Since the refurbishers of Griffin-Floyd did not insulate the walls or replace the windows, the savings can not come from this building. Chilled water outages also occur, but those are usually planned and well announced. The fire alarm is also occasionally tripped by students evading tests, and this shuts off the AC.

### **7.1 Remediation**

When the AC fails the temperature in the server closet does not go above 90° F. This is undesirable, but within specification. Some servers newly taken out of service will soon be switched off, which will lower the heat load and reduce the maximum temperature. There used to be a machine which would page the sysadmin when the temperature went too high, but this machine was one of the ones just taken out of service due to age. Replacing the temperature alarm feature is in the works. Two fans exist to be used when the AC is off, and opening the doors and setting the fans helps quite a bit.

## **8 Risk: Plant problems you can't ignore until morning**

- Front office door won't lock
- Front office window is broken
- Chilled or hot water leak is streaming out of the attic
- Vandalism discharge of fire extinguisher (corrosive dust hazard to computers).

### **8.1 Remediation**

There are PPD folks on call including a locksmith and a HVAC plumber. Call PPD, have them page their on-call, wait to do a handoff.

UPD can provide real physical security in the middle of the night, and probably wants to collect undisturbed evidence on a physical breakin anyway.

## **9 Risk: Disgruntled ex-user who may attack computers**

### **9.1 Remediation**

Terminate their access in a quick and positive manner, with multiple overlapping changes, and don't worry about elegance. Examples: `chmod` their home directory to 000, then rename it. Kill all their processes on all machines. Pull the network cable on the NFS server if an attack is in progress. The sysadmin has better access than a user does, and this advantage should be used and retained.

## **10 Risk: Sneaky dishonest user breaking security**

- Selling tests
- Stealing research
- Stalking users
- Identity theft for whatever purpose

### **10.1 Remediation**

Confer with computer committee, so academic consequences can be coordinated with civil and criminal ones. Don't lose or contaminate evidence. Keep copious notes, and expect them to end up in court. Involve police sooner than later. Keep everything aboveboard.

## **11 Risk: Server data loss; partial, progressing, or total**

- Disks fail; more often incrementally, sometimes all at once.
- Sysadmins have accidents

## **11.1 Remediation**

At least one copy of all unique files is in the TSM backup system, except for logs and data in-flight on the desktops, which are not considered worth the price of backing them up. Within the depth and frequency of TSM coverage for which we have chosen to pay, anything can be either recovered from backup, such as servers, or recreated by a semi-automated process, such as desktops. Data recoveries used to get tested end-to-end rather a lot, as machines were well past their design lifetimes and hardware was failing. Newer machines mean that fewer disk failures are generating backup tests, but the backup system has not been changed since its period of intensive testing. Additional spot checks occur when the TSM system is used as a temporary storage space for system administrative convenience, mostly during machine rearrangement.

The continued operation of TSM backups is verified from both ends. There is a daily report of transfer volume on the department side, and a daily report from the TSM administrator about any machines TSM is aware of but hasn't been heard from recently. These reports go to a campuswide community, so if the sysadmin is hit by a bus someone will warn the department of lapses in backup coverage.

It is possible to put a server into service but never back it up. The monitoring is intended to catch mistakes, surprises, and hidden failures, not basic procedural flaws.

## **12 Risk: User deletes something they wanted**

Now, where did I put that paper containing my irreplaceable research data?

### **12.1 Remediation**

The TSM features described under Section: Risk: Server data loss apply if the deletion is caught in a day or two. There is also a rotating tape archive made weekly of home directories which goes back a few months, so that there is a good chance of recovering missing or damaged user files that are not discovered immediately and expire out of TSM.

## **13 Risk: How are the network wires arranged?**

### **13.1 Remediation**

At the end of the recent building rewiring, we documented a completely accurate network wire map as we installed the patch cables, and since then we have documented changes religiously.

## **14 Risk: What hardware do we have?**

### **14.1 Remediation**

We keep the Property Services asset database usefully up to date, more up to date for what we have than what room it is in, and we have access to a scanner-person from the college after bulk machine installs or trickledowns. We've backfilled the important missing data like serial numbers.

## **15 Risk: Password guessing**

### **15.1 Remediation**

New users are assigned passwords made of entirely random characters, and then strongly discouraged from changing them by making changing a manual, personal process with the sysadmin.

## **16 Risk: Network sniffing**

### **16.1 Remediation**

There are no protocols within the department in which passwords go over the net in cleartext. The non-encrypted IMAP port is turned off to prevent user configuration mistakes at home from using it and revealing their passwords. Outgoing mail submission goes over SSL with mandatory authentication so as not to be an open relay; however, plaintext authentication is rejected if SSL or TLS is not already active in the session.

## **17 Risk: Stale Accounts**

### **17.1 Remediation**

Users who depart on good terms must find a faculty member to sponsor their continued use, if they have a reason to retain their accounts.

## **18 Risk: Privileged access**

### **18.1 Remediation**

Department-controlled Windows machines offer power user access to install software, as a tradeoff between security and convenience that does not provide a trivial path by a naive user to impersonate other users or access their materials.

Any login or activity by a privileged user is logged and auditable to the extent that the vendor offers such features. The logs on Linux are quite good should the attacker not understand how to falsify them.

## **19 Risk: Authorized remote access**

### **19.1 Remediation**

Authorized remote access is only available through a few select and hardy protocols, such as ssh, encrypted email, and encrypted webmail.

## **20 Risk: Social engineering**

### **20.1 Remediation**

When a particularly well-written phish comes through, we warn all our users to ignore it.

## **21 Risk: Physical access**

### **21.1 Remediation**

The computer lab has a combination lock on the door, which prevents outsiders from wandering in. The doors to the server closet and the network switch closet are locked to general userdom.

By design, there are no situations in which a user opening the case of a department-maintained computer or rebooting it under another operating system would be even faintly justifiable. This permits the presumption that anyone caught exploiting physical access to a machine has bad intent.

## **22 Risk: Loss (theft, damage, etc.) of computers**

### **22.1 Remediation**

Computer hardware warranties are purchased in the longest lengths available, nowadays 4 and 5 years. This protects against hardware failure for the obsolescence life of the equipment.

Equipment is stored behind locked doors, which means physical security is no worse than the the general tradeoffs made for locks and keys on campus.

Serial numbers are recorded in the Property Services asset database in case taggable-value equipment is stolen.

## **23 Risk: Licensed software**

### **23.1 Remediation**

We make a point of purchasing all the software we use. Manual audits of Windows are too expensive to do, but we do know who is supposed to have copies of what.

The request to install licensed software in a new location generates a purchase transaction. As cheap as it is, the user isn't asked how they want to pay for it, it's just bought. The few expensive software packages like Linux SAS generate enough budget angst that they get plenty of oversight.

Most Windows software is site-licensed through James Hardemon's group at <http://www.software.ufl.edu> to get good prices, and most of it activates against on-line licensing servers. This makes it trivially unusable if it is given away. Most software has home-use provisions, and this removes the biggest cause of cheating on licenses.

Within some accuracy bounds it is discoverable how many average simultaneous copies are running in the department, and this number is reviewed by Hardemon in the yearly reapportionment of license costs.

## **24 Risk: Personal laptops**

### **24.1 Remediation**

The biggest ongoing problem with Windows laptops used to be them attacking campus, despite an ironclad policy of virus scanner installs and virus scans before a wire connection was granted. This was solved by shifting their connections to wireless.

DHCP on the wired network is not handed out to unknown ethernet addresses. Users cannot accidentally or innocently get a wired connection. Meanwhile, the wireless environment was brought up to reasonable performance everywhere by adding a second access point on the first floor.

Authentication over encryption for email coming and going means that the same set of email server settings will work no matter what network the laptop is moved to, be it a home address that we might be able to learn, or a distant one we would not. This has made traveling with a laptop a much more pleasant experience for users.

It is surprisingly easy to navigate the Windows wireless connection menus by position, even if the menu entries are in Korean or Chinese.

## **25 Risk: Private machines**

### **25.1 Remediation**

Private machines are only allowed on the wire as special cases run by highly knowledgeable users. Everything else is connected via wireless. This distinction is meaningful because any service that is not intended to be broadcast to the Internet at large is limited to the building public IP address range, if not limited further.

## **26 Risk: Server closet and desktops physically destroyed**

### **26.1 Remediation**

With the new TSM mirror site in Atlanta, TSM backups are beyond the reach of plausible physical destruction scenarios, such as a big fire, big tornado, or someone running amok. Since the data is safe, the question becomes how soon can it be restored and made available, onto what machines, housed where?

If only Griffin-Floyd is lost, web and email will be redirected onto existing servers provided by the charity of the college, and users will use their laptops over wireless and their personal cell phones. Secondary DNS and mail server queuing will bridge the time window until the new services are working. The college will provide alternate office space in some manner. The college is not expected to replace the entire departmental computing infrastructure.

If the Northeast corner of campus is lost, users will retreat to their laptops and existing email and web space accounts they have for personal use. Geographically distributed operation from home is a possibility. If the VPN is unavailable, it is an unanswered question how to maintain access to online journals, JSTOR, and pool-licensed software without a UF IP address to use for a license key.

A loss of more than the Northeast corner of campus is out of scope for this plan.