

Back It Up: Safe IT Practices

by Philip Chu

Table of contents

1 Publication Information.....	2
2 Trust, then Verify.....	2
3 Be Redundant.....	3
4 Have a Plan.....	4
5 Know the Applications.....	5
6 Know the Business.....	5
7 Know the Rules.....	6
8 Communicate the Policy.....	7
9 You Can't Take It With You.....	8

1. Publication Information

Copyright ©2004-2007 by Philip Chu All rights reserved.



IT is getting harder every year, due to the march of technology, increasing spam, and more nefarious security attacks. But there are some basic principles in taking care of your organization's IT needs, whether it's a one-person shop or a huge corporation.

2. Trust, then Verify

Backups are like insurance policies - you don't realize how much you need them until you really need them. It's not enough to have a backup system - you need to have assurance that it

will save you when you need it to.

- An owner of a small game development company assured me that all important data was backed up periodically. It turned out this didn't include our source code. Even after this was rectified, the backup tapes were never verified, and a server crash lost a month's worth of work just before E3 (the big trade show).

Complacency isn't limited to small companies. When I worked at a large research institution that operated the Hubble Space Telescope, the army of college students running nightly backups looked reassuring until one of my coworkers lost a file and found the backup was unreadable.

It's not enough to just make the backups. If you don't periodically verify that you can restore from the backups, there's not much point. In a similar vein, keep your backups offsite. If your office is ransacked or goes up in flames, the backups won't help if they happen to be sitting in the same room.

- This was my first practical on-the-job lesson. An experienced, high-level engineer was brought on to my project to help get things organized, and the first thing he did was shop for a fireproof safe and offsite storage space.

Regular backups are considered standard IT procedure, yet paranoid programmers like myself often feel it necessary to make their own backups just in case. At one small company, I was so distrustful of the backups (rightfully so - we eventually had a server crash just before a trade show and the backup tapes were unreadable), that I bought my own backup drives and media. But you don't want to rely on your staff to protect your data and in general you don't want them taking company data home (at least not just for backups). So do it right yourself.

3. Be Redundant

Management is often reluctant to spend a lot of money on hardware, especially given the inevitable obsolescence. But the cost of hardware pales in comparison to the salaries of programmers sitting idle because their workstation died and there's no immediate replacement, or the cost of a project delay due to a wait for critical equipment.

- Fortunately for me, in recent years I've been on projects where lack of hardware and software was not an issue. But the early part of my career was spent in large corporations and government projects where you had to jump through hoops to get the resources you needed to complete a project. I remember one military project where I was directed to order a new hard drive as "laboratory equipment" since we had more funds in that budget. The on-site naval representative responsible for vetting all such expenditures didn't seem

to agree that was the correct categorization, but rather than immediately denying the request, he responded with requests for increasingly more information - what laboratory? what experiments will the hardware be involved in? submit a wiring diagram of the lab indicating how the hard drive will be connected!

You also want redundant knowledge.

- The first startup I joined that really felt like a startup had no dedicated IT person. My office space was a spot on the floor and we all set up our own computers. My manager was surprised when he saw me swapping tapes while the regular backup guy was on vacation, but really, neither skipping backups or denying vacations are good options.

At another startup that wasn't quite as well funded, the air conditioning was off on weekends and evenings, including in the server room. It's a good thing I was shown how to restart the server - on summer weekends our IT person would call the office and say the server was apparently down, could someone reboot?

Make sure your IT person can go on vacation without the company grinding to a halt.

4. Have a Plan

Just as with software development, and for that matter, any other functional department of a business, there should be a long-term IT plan. Solely reacting to near-term needs will make transitions to future operations inconvenient, if not impractical. Think about how many users you will have to support, security and application needs, and future services that will have to be supported, and how much it will all cost.

- I was on a game project that had an excellent infrastructure consisting of cutting-edge third-party and custom development tools and a large, responsive IT staff. But just as things were getting busy and more development staff was added to get the project done on time, we got bogged down using the asset management tool - the number of licenses available were inadequate to keep everyone working simultaneously, and it took several weeks to acquire new licenses.

One tool that makes a difference between a run-of-the mill IT group and a top-notch group is a ticket system.

- I spent a good portion of my early career hanging out in IT offices and server rooms. Not just because I enjoyed their company and the air conditioning, but it seemed to be the best way to make sure they wouldn't forget my requests. When dealing with IT groups that employed ticket systems, in the worst case I could call up and refer to the ticket - in the best case, I had immediate responses over email and sometimes an immediate visit at my desk.

5. Know the Applications

It amazes me that IT often doesn't know the first thing about the applications it installs. Admittedly, I often can barely use the programs I develop, but still, I can at least launch them and invoke rudimentary operations. On the other hand, I've seen IT personnel unable to run the programs even to verify their successful installation.

- At one game development company where we had contract IT support, we had an ill-timed switch of our logins to new domain-based accounts over the weekend. Not only was this without advance notice, leaving people wondering on Monday why their original accounts were not functional (in particular, email, so there would have no point in notifying everyone by email after the fact), but many of the applications installed in the original accounts did not function in the new accounts.

This fiasco occurred because the IT contractor was familiar with everyday-use applications like Microsoft Office and was apparently confident those packages were transitioned correctly, but was completely unaware that as software developers, we used quite a few other programs that were critical to our business, like compilers. And apparently the person managing our outsourced IT failed to consider that, too.

The same IT contractor also went the extra mile to install virus-scanning software on all our machines and enabled them, again without telling anyone. And again, this is a good idea for normal computer usage, but many software code generation tools are documented not to play well with virus scanners.

Moreover, with dependencies and interactions (read, bugs) with different drivers, multimedia capabilities (e.g. versions of DirectX) and operating system versions and patches, it is important for IT to track issues with the critical applications used by developers.

6. Know the Business

IT procedures have to be in sync with the company's business. Practices adequate for maintaining regular 9-5 businesses may not be compatible with software development houses, Internet operations, or financial institutions.

- The aforementioned switch to domain-based accounts at a game development company not only went badly, but took place during the final crunch time stretch for that particular game. Remarkably, this happened again a year later at the same company with the same contractor - a new router was installed, once again without notifying anyone in advance, and worse yet, this was the morning of a business day, and once again during crunch time development. Considering that the employees were asked to put in extra hours in the

evenings and weekends, this was really unforgivable.

When involved in packaging products, IT needs to know the application requirements and how to manage configuration changes.

- Another game company I worked at developed arcade games running on stock PC hardware. Our testers discovered a graphics glitch just as some new machines were being packaged for delivery overseas, and upon investigation it turned out that our hardware vendor had stopped offering our the graphics card used in our configuration, so our PC configuration people had started ordering a different card without considering that our game might not run correctly with it.

And in some cases, particularly web-based services, IT is on the front lines with the customer and should be acquainted with customer needs and expectations as much as anyone else in the company.

- One of my favorite projects was a wireless web browser and gateway for handheld devices. But for a consumer service that was supposed to run 24/7, we ran it haphazardly. After some heated discussions with my managers about adding features in before the launch date, I discovered our IT manager had already launched the service at his own initiative, with little fanfare. And when we moved our office upstairs for more space and a nice view of the San Francisco Bay, the gateway machines were moved in the late afternoon with no advance notice to customers or even staff. Any Friday afternoon commuters who wanted to browse the web on their train ride was out of luck.

It's not just small startup companies that get this wrong. I'm amazed in this era of Web 2.0 how badly prominent web sites are run.

- I was an avid review writer on Epinions until I lost several reviews-in-progress on Sunday afternoons - that is when when they scheduled their site maintenance update. Even Google showed some amateurish site management - I delayed setting up my AdSense account for a week because the password-retrieval page was down. The worst case I've seen of a site-that-should-know-better was the local Time-Warner cable broadband signup page. For at least a week the page stated it was down while an update was in progress, and for a while after that, it displayed the startup Apache server test page. If there was a truly competitive broadband market, imagine how much business they could have lost?

7. Know the Rules

Like HR, IT is part of every employee's tenure from day one. The rules don't just involve proper IT ticketing procedures. These days, every employee, and thus every IT practitioner

should know the legal requirements and corporate policies governing privacy and proper use of the IT infrastructure.

- I worked for one delightful employer who went into muckraking mode whenever an employee left or was terminated - she would scour the former employee's hard drive and announce to everyone she found porn and lascivious email. Eureka!

Employees should know what expectations of privacy they have, who owns the data on the computer they're using, and what activities, e.g. porn-surfing, are restricted. (Although a friend of mine pointed out that some occupations are so thankless, Internet porn should be considered a job perk)

Management should also know, or be informed, if they're clueless, what lines they can't cross.

- In one of her more vindictive moods, the aforementioned employer floated the idea of breaking into a former employee's Yahoo webmail account, apparently assuming that was fair game if that account was accessed from work. It's not.

And you can't depend on the company legal department for expertise.

- While wrangling over a contract with a large video game company, I complained to their legal department that one of their clauses made no sense - it stated that any licensed components that I built into a deliverable would have to be sublicensed by me to them without restriction. This indicated ignorance of how software is constructed (e.g. just building an installer typically incorporates installer code from the installer vendor) and how software licensing works (or even what the word "license" means). Ever read one of those interminable EULA's?

8. Communicate the Policy

Defining proper and improper employee behavior is always a tricky business, and computers in the workplace make it even more so.

- Terminating an employee is often a messy scene involving weeping, yelling, begging or all of the above. But sometimes what happens afterwards the employee leaves the premises for the last time is worse. People descend on that person's computer and discover porn, evidence of freelance work, and even sometimes root through email (one of my employers read an ex-coworker's email to his girlfriend)

You could argue that employees shouldn't make any personal use of office computers and anything they leave is fair game for employers who have to protect their interests. You could argue that it is in poor taste and unethical for employers to gratuitously root through all the

leavings. Either way, make the rules clear - that's what employee handbooks are for.

9. You Can't Take It With You

The IT relationship with an employee doesn't end with his departure.

- One of my employers laid off several employees in a Friday afternoon massacre, notifying them at 5pm. One said he didn't have time to clear out his office and would have to return later to do that, including retrieving information from his computer. As this obviously was not a trust-filled working environment, the employer worried that this newly-disgruntled newly-ex employee might do some damage on the network. My suggestion: as a regular practice, as soon as an employee is terminated, back up that computer, save a snapshot of the final state on CD, DVD or whatever for easy access later, and take the computer out of service.

Taking snapshots of departing employees' hard drives is also a good practice for less cynical reasons. If the engineering team has to call up the employee and say "Hey, where is that documentation?" or "Did you forget to check in that last bug fix?" you're not out of luck.