

Even dirtier IT jobs: The muck stops here

More dirty tech deeds, done dirt cheap

By Dan Tynan

Hey, we can't all have careers at Google. Sometimes when you work in IT, you have to hold your nose and hope for the best.

Last year we named "The 7 dirtiest jobs in IT," but we barely scratched the topic's grime-caked surface. In the world of technology, there's plenty of dirt to go around.

You may be ordered to crawl into the nastiest corners of your office – or to explore the nastiest corners of the Web. You may be required to stare zombie-like at a network monitoring console, waiting (possibly hoping) for the alarms to go off, or be chained to an endless series of spreadsheets

and Word docs, looking for minute differences in data. You may end up berated, belittled, or sobbed at for circumstances that have nothing to do with you.

And at some point in your IT career, you will probably be asked to spy on your fellow employees – or even your boss – and fearlessly report what you find.

These seven jobs are not for the faint of heart or the weak of stomach. But they're out there; in these dark economic times, you might consider yourself lucky to have one of them.

Dirty IT job No. 7: Disconnect/reconnect specialist

Wanted: Able-bodied individuals with affinity for adapters, plugs, prongs, and dongles; willing to crawl under desks and squeeze into tight spaces that have never seen daylight. Strong stomach required.

Disconnect machines from one site, reconnect them at another. It sounded so simple Garth Callaghan couldn't quite believe someone would pay his company, **I27tech**, to do it. Now he employs three full-time employees and 30 contractors, who spend half their time unplugging and replugging machines for commercial movers in Richmond, Va.

But don't think they don't earn their money.

Most businesses have been in the same location for a long time, says Callaghan, and many of their employees haven't budged from their desks in 5 or 10 years. That can make for a rather mucky experience.

Occupational hazards include dust bunnies the size of basketballs, displays coated in soot, keyboards with enough food lodged in them to feed a small third-world country or, in one recent case, caked with a viscous layer of cosmetics.

In the three years his company has been in business, Callaghan and his crew have probably unplugged and re-plugged 10,000 workstations. But one in particular stands out.

"One day a couple of years ago, one of my crew members was struggling to get some cables loose from between a workstation and a wall," he says. "I said, 'Don't worry, I'm the owner of the company, I'll take responsibility if the cable breaks.' I grabbed the cable and started to shimmy it up. It wouldn't budge. Finally I yanked really hard. Out popped a bottle of Italian salad dressing, three-quarters empty. It had leaked all over the wall, the desk, and the computer. When I looked at the label I saw it was two years past its expiration date."

Callaghan says that while the experience did not put him off Italian dressing, it will be burned in his memory forever.

"My entire crew has to shower down after our job," he adds. "It's not quite 'Silkwood,' but sometimes it feels that way." »

Dirty IT job No. 6: Data crisis counselor

Wanted: Empathetic individual able to withstand long bouts of unwarranted abuse; soothing phone manner and low blood pressure essential.

When disaster strikes and critical data goes down the memory hole, it can generate a gamut of unpleasant emotions – tears, depression, guilt, hopelessness, and rage.

It's Kelly Chessen's job to listen to it all. As a crisis counselor for data recovery firm DriveSavers, she's gotten calls from sobbing adults who've lost images or videos of their recently deceased parents. She's talked to dentists who were frantic because their systems went down and they have no idea what services their patients needed. She's logged hours with IT managers who lost entire Microsoft Exchange servers because they thought they knew how to implement RAID 5 but really didn't. Now their servers were dead, the backups were missing, and their jobs were on the line.

"I would talk to one IT guy one day and another IT guy from the same company the next day because the first guy had been fired," adds Chessen, whose job title really is Data Crisis Counselor.

Though she has an undergraduate degree in psychology, it was Chessen's five years on a suicide prevention line that best prepared her for her current position, which she was offered after a chance encounter with the president of the company. (No, he was not one of her callers, she hastens to note.)

Chessen says the worst call she ever received was from a small-business owner whose building had burned to the ground, taking all his computers with it. "He yelled at me for 30 minutes straight," says Chessen. "I didn't burn down his business. But after 5 or 10 minutes of yelling, it's hard not to take it personally."

It's a job your average IT person would be wholly unsuited for, agrees Chessen.

"Not everybody can do what I do for living," she says. "You need the skills, the background, and the patience. It's a dirty job, but it's also very rewarding, because we have a solution. In almost every case, we can get their data back for them, sometimes as quickly as 24 hours."

And on those rare instances when DriveSavers can't recover someone's data because the drives are simply too far gone? "I do grief counseling," she says.

Dirty IT job No. 5: Fearless malware hunter

Wanted: Go-getter with inquisitive nature and a high tolerance for gore, sleaze, and the baser instincts of humanity.

Hunting malware means crawling the deepest, darkest, nastiest corners of the Web, because that's where the bad stuff usually congregates -- such as drive-by installs on porn and warez sites, says Patrick Morganelli, senior vice president of technology for anti-malware vendor Enigma Software.

"Due to the nature of the sites we need to monitor, one of our first questions in any job interview here is, 'Would you mind viewing the most offensive pornography you've ever seen in your life?' Because that's what a lot of malware research entails."

Even employees not actively involved in malware research can encounter deep nastiness, he says. One time an employee merely passed by a support technician's display while the tech was remotely logged in to a customer's PC. What the employee saw on the tech's screen was so disturbing that he quit shortly thereafter.

"It can definitely wear on people," Morganelli says. "The amount of filth you need to go through on a daily basis just to do your job can be pretty trying, and much of it is extremely disturbing -- bestiality and worse. But there's no way to fight this stuff unless you go out and actively collect it."

Andrew Brandt, a malware researcher and blogger for security software vendor Webroot (and InfoWorld chronicler of IT admin gaffes, stupid hacker tricks, and colossal QA oversights), says he was warned before he took the job that he'd see porn that would turn his stomach. But he says he sees less malware distributed via porn sites and more via fake BitTorrents and game cheats sites.

"I would describe my job as rubbing a white glove on the filthy underbelly of the Net and seeing what comes off," says Brandt. "Every day I work with malware that does everything you don't want it to do -- like steal your bank account information, break your computer, or barrage you with ads -- and I do it 20, 30, 40 times a day."

"The dirtiest thing about my job is not that the malware is incredibly difficult to research or fix; it's that once the bad guys latch onto some trick they use it over and over and over. I start to crave the little differences that crop up. Still, every day I learn something new -- even if it's just 'oh my god, this is the hundredth time I've seen the exact same exploit.'"

Dirty IT job No. 4: Zombie console monkey

Wanted: Individuals with low self-esteem and high boredom threshold willing to spend long hours poring over server logs and watching blinking lights on a network console.

This job title combines two of the most onerous yet often necessary tasks ever assigned to an IT grunt: analyzing system logs and monitoring network operations, says Lawrence Imeish, a principal consultant for IT services provider Dimension Data.

"Doing log file analysis and correlation has to be the most tedious, mundane, perpetually boring job in of all IT," he says. But because logs maintain detailed records of all activity that takes place on a system, they're vital tools for debugging and error detection, he adds.

"Meanwhile, network operations centers usually have a person whose job is to stare at screens waiting for green lights to turn red, signifying a problem with some system," he says. "There are useful messages in all those blips and flashing lights, though, and many of them can go a long way toward preventing problems before they occur."

As companies trim body counts, they often combine these positions into what Imeish calls the Zombie Console Monkey. The utter lack of human interaction combined with little to no exposure to the sun means Zombies have been known to become almost transparent over time, he adds.

These days, mature IT organizations use event correlation software and network monitoring apps that can identify anomalies and notify the necessary parties if the network fails. Even then, says Imeish, some companies feel more comfortable with a human being sitting there and watching the dials, just in case.

"It's an entry-level job with not a lot of thought involved. Creative thinking? Forget about it. Your job is to follow a script, written down in a manual, for anything that might happen. That's why we call them 'zombies' -- no brains are required."

Dirty IT job No. 3: Data cleansing drone

Wanted: Detailed-oriented individual to pore over endless amounts of repetitive data looking for errors. Requires high tolerance for mindless drudgery; clinical diagnosis of obsessive-compulsive disorder a plus.

Data is a harsh mistress. The same name spelled two different ways or slight variations ►►

in addresses can wreak havoc with your inventory, screw up your billing, break the supply chain, make customer service a living hell, and cause the suits to make bad decisions. That's why thousands of organizations hire drones to comb through company files looking for inaccuracies, inconsistencies, discrepancies, duplicates, and other data glitches.

"We call it the 'Monk factor,'" says Stefanos Damiakis, CEO of Netrics, a maker of data matching software. "Like the detective in the 'Monk' TV show, every organization has obsessive-compulsive guys who pore over the data and try to make it perfect."

Forget perfect data. Getting the data to where it's usable is hard enough, he says. "The job is dirty because the data is relentless. You're just sitting there looking at the same things over and over. It's mind-numbing, and the tools available to do the job are typically antiquated."

Even if the data is consistent across all fields, organizations still need people to figure out what it really means, says Leonard Dubois, senior vice president of marketing and sales support for Harte-Hankes Trillium Software, maker of data quality solutions.

"In large organizations there are hundreds of people poring over Excel spreadsheets and Word documents trying to determine what the business meaning of a specific term -- like 'customer' -- might be," says Dubois. "And every silo in the organization might have a different definition. If I order a book from Amazon for my wife, who's the customer? To the billing department, it's me. To marketing, it's my wife. To shipping, it's the address where the book got sent."

The data drone has to go in and figure out which definition is the correct one for each group -- an expensive and time-consuming process. Data quality software like Netrics' or Trillium's can automate many of these tasks, detect errors, and reduce guesswork. More often than not, though, you still end up with outliers that have to be handled by humans.

"They call it data cleansing for a reason," Dubois adds. "It's a tedious process to go through data files and figure out the meanings of each term."

Dirty IT Job No. 2: IT mortician

Wanted: Morbidly minded individual sought to gather up dead or discarded electronic equipment and perform last rites; excavation and embalming experience preferred.

In every organization there's always somebody who has to go in and deal with the dead parts of IT -- whether they're reclaiming

infrastructure from companies that are no longer in business or simply disposing of machines that are too old to use, even if they're not quite dead yet.

As with disconnect/reconnect specialist, the job can be literally dirty, says Dimension Data's Lawrence Imeish. "This stuff can be pretty disgusting," he says. "You're dealing with years of dust, grime, and neglect. A guy gets back from one of these jobs, you'd think he worked in a coal mine."

Sooner or later, someone will demand you take possession of their "extremely valuable collections of IBM AT look-alikes, Pentium-I knock-offs, and 'does 386 sound familiar?' artifacts from the Mesozoic era," says Bill Horne, a systems architect with William Warren Consulting.

Horne says he patiently explains that the best resting place for such systems is a local charity that will take them off the company's hands without charging a recycling fee, but most clients remain unconvinced.

"You'll be rewarded with angry demands to remove them that very minute, no matter what you thought your plans were for that day," he says. "The rear surfaces of at least one machine will be razor-sharp, and that's the machine you will make the mistake of grabbing as it starts to fall off the shelf where it was balanced precariously for centuries."

Worse, every machine will have at least one virus on it, and the software will be unsalvageable. "The best you'll be able to do is get a couple of 'free' Windows ME serial numbers," says Horne. "But you'll have to resign yourself to your fate, put bandages on your hands, wipe the blood off the face plates, flatten the hard drives, and deliver them to the Disabled Veterans' collection point."

Dirty IT job No. 1: Espionage engineer

Wanted: Network sleuth willing to secretly read employee e-mail, shadow coworkers across the Web, and unmask corporate spies; ability to keep secrets a must.

Work in IT long enough, and one day you may be asked to monitor your fellow employees' e-mail, scan their browser histories, or rifle their hard drives looking for evidence they've broken the rules. It's just a fact of doing business, says Roger A. Grimes, a senior security consultant and proprietor of InfoWorld's Security Adviser blog.

"I'd say it happens in 100 percent of large and midsize organizations, less often in smaller ones," he contends. He estimates that half the time employees who are investigated ended

up being fired. Only about one in four prove innocent.

The biggest single issue Grimes is asked to investigate? Sex between two employees. "That accounts for 50 to 75 percent of the requests," he says. No. 2 on the list is corporate espionage, usually in the form of soon-to-be-former employees absconding with proprietary company data.

At one company, Grimes discovered that nearly half of the network Web traffic was porn-related. When he informed the CEO, he was gently dissuaded. "We don't want to be the Internet police," he told me.

Grimes immediately looked at the CEO's hard drive, where he found a generously endowed cache of gay porn, as well as evidence the executive had booked a session with a male prostitute on a business trip to Miami. At the time, the CEO was days away from getting married.

Two weeks later, the CEO called him into his office. "He said a couple of teenage boys had broken into his home and surfed gay porn on his computer, and now he wanted to know how to get rid of what they left behind," Grimes said.

Shouldn't the chief executive call the police? Grimes asked. No. He just wanted to know how to clear his cache. A few weeks later, the marriage was officially over.

The CEO was hardly the only one in that company caught with his hands in the, umm, cookie jar.

"I could prove a large percentage of senior management did no actual work at all," says Grimes. "These guys were making several hundred thousands dollars a year, and all they did all day long was surf porn."

But being an IT spy is not all fun and games. Grimes says he's been approached by spouses of executives seeking evidence their significant other had been cheating. He has to tell them no, he can't legally do that. Over the years he's also investigated dozens of employees charged with viewing child pornography at work.

"I try hard to not find images on people's computers," he adds. "There are some things you simply can't unsee. It's an emotionally difficult thing to be involved with."

Sometimes, however, it's hard to avoid.

"One time I was asked to clean off the computer of an executive who was leaving the company," says Grimes. "She was in her sixties, with gray hair. Going through her hard drive I found pictures of her in leather bondage with another executive at the same company. I just deleted them. But I never could look at her the same way after that." *