Published on *InfoWorld* (http://www.infoworld.com)

Eight is enough! IT's biggest frenemies

By Dan Tynan
Created *2013-06-10 03:00AM*

You probably have a good idea about who your enemies are. But what about your frenemies?

These are people you deal with on a regular basis, largely because you have no choice. But even when their intentions are good, they can still cause you all manner of grief. They range from BYOD Betty, who insists on using her iPhone at work (but wants you to support it) to Cloudy Claudette, who's running her own shadow IT organization with the help of public cloud providers.

[Learn the 8 biggest myths about managing geeks and how to repair dysfunctional IT relationships. | Also on InfoWorld: Beware the nine circles of IT hell, and steer clear of 20 common IT blunders and IT's 12 worst "best practices." | For the latest in technology news and analysis, sign up for the InfoWorld Daily newsletter.]

It could be Pedro, the work-at-home manager who never takes off his pajamas but expects tech support to be at his beck and call 24/7, or Leaky Louise, who also brings work files home, until she inevitably loses them. You might work with Frightened Frank, the chief security officer whose vocabulary consists of a single word ("no") or HR Harriet, the human resources head who makes hiring even more hellish than it should be.

And if Legacy Larry is your CEO, you might still be using hardware or software that hasn't been updated since the grunge era.

The biggest problem with frenemies is that you have to work with these people. You might even have to be nice to them. But while you may never end up BFFs, you don't have to put up with all their shenanigans. Here are eight common frenemies and how to keep them in check.

IT frenemy No. 1: Legacy Larry
The new senior manager with the perfect cure for your IT woes -- and it's only 20 years old.

You know Larry. He's the new boss who's brought his favorite tech tools with him -- the same ones he used at his last job and the one before that. Now he's decided that everyone has to use them. Larry can also be the CEO who'll cling to old technology "as long as it still works," no matter how paleolithic or performance sapping it may be.

Anthony R. Howard recalls having to convince one Legacy Larry to replace the 15-year-old 10/100Mbps switches in his network with newer 10-gigabit models.

"I told him, 'I remember this model; it came out when I was in college,'" says Howard, a best-selling author ("The Invisible Enemy: Black Fox") and independent technology consultant for Fortune 50 companies and the U.S. military. "'Technology has come a long way since 'The Matrix' came out, Larry. Your network is now running 100 times slower than it should be.'"

Robert King, principal of management consulting firm EntelliProj, was working with an organization in the mid-2000s built around Microsoft Exchange. A newly hired senior manager convinced the board that Lotus Notes was the collaboration tool of the future. After nearly two years, a steep learning curve, and a vast expenditure of IT resources, Notes was fully deployed -- just as Microsoft SharePoint began getting traction in the marketplace.

"One of my pet peeves is senior decision-makers who are indebted to a specific technology and want to implement it in every company they pass through, without regard to cost, training, change management, or employee morale," says King. "What worked for organization A won't necessarily work for organization B just because an executive changed jobs."

How to keep them in check: You can start by pointing out how much the legacy solution is costing the company, says Howard.

"A savvy supplier can get you new equipment that's cheaper than maintaining the old gear," he says. "You just have to show Larry this in a way he understands it, using dollar signs. Put it in terms of risk, disadvantage to competition, cost of maintenance, energy usage, and lost productivity."

And if management still insists on using aging technology?

"My advice is to accept that and try to get it to work as best you can," says King. "If IT continues to resist, it will end up being devalued by senior management and lose influence."

IT frenemy No. 2: BYOD Betty
No need to supply Betty with mobile technology; she's bringing her own. What she's also bringing: A support and security headache.

Betty may be constantly on the go, but she's never very far from her iDevice. Of course, if she runs into problems, she'll expect IT to support it, just as Android Alex and BlackBerry Bob do. And if her baby gets lost or stolen, well, let's hope there's no sensitive company data on it.

The beauty of BYOD is it enables employees to be productive from virtually anywhere with minimal up-front costs for the organization. But Betty and her cohorts aren't making any friends in the IT department.

"Each new tablet or smartphone platform introduces added complexity for IT," says Nathan McNeill, chief strategy officer for Bomgar, makers of remote support software. "Not only are reps tasked with troubleshooting them when something goes wrong, they also need to develop -- and support -- applications that work across different mobile operating systems."

How to keep them in check: Trying to keep people from using their own tablets and smartphones at work is a battle you are likely to lose. But you can take steps to minimize the pain of BYOD. Instead of trying to become experts in all mobile devices, McNeil says, tech support should try to bring in power users with OS expertise to help handle issues as they arise.

As for securing BYOD gear, it's ultimately no different than securing devices distributed by the enterprise, says Tsion Gonen, chief strategy officer for security firm SafeNet.

"You start by creating a simple policy that says you can use your phone at work so long as you don't rootkey or jailbreak it," says Gonen. "After that, it's just basic stuff -- encrypt the data, enforce a serious password, and enable remote wipes of lost devices. It's not rocket science. People want to be compliant; you just need to tell them how."

IT frenemy No. 3: Pedro de las Pajamas
Because he's special, he gets to work from home. And because he's constantly having tech issues, you get to work from his home, too.

Though he's rarely seen around the office, Pedro's no slacker. He gets his work done without anyone standing over his shoulder. Thanks to Skype he never misses a meeting. And because there's no separation between his home and work life, he'll respond to urgent emails and texts after most of his colleagues have clocked out for the night.

But Pedro can be a support nightmare, especially if he lives and works in a different time zone than other employees, notes Bomgar's McNeill. He may also be using devices and applications not officially sanctioned by IT, posing potential security or compatibility problems.

"Remote workers need just as much tech support as those in the office, but they can cause more headaches," says McNeill. "If they're located in different time zones, you need members of your support team available during those hours, regardless of how inconvenient that may be."

You start to understand why Marissa Mayer banned them from Yahoo.

How to keep them in check: Having secure remote support tools are critical for helping frenemies like Pedro, McNeill says. You'll also need education materials on hand so that remote workers can get up to speed on company procedures and technologies on their own.

"Supporting remote workers requires IT to be constantly one step ahead," he says. "You need to anticipate challenges before they arise while also ensuring the tools they're using to assist these employees are not exposing the company to serious risks."

IT frenemy No. 4: Leaky Louise
She was only taking work home -- she didn't mean to lose that thumb drive with your entire client list on it.

Louise is nothing if not dedicated to her job. Every night, she religiously loads data onto a USB drive or emails files to her personal account so that she can catch up on work after dinner.

Though technically against company rules, nobody seems to care -- and it's for the good of the business, right?

Nearly half of all employees take company data home with them at least once a week, according to a February 2013 survey by Symantec and the Ponemon Institute. One-third of all companies surveyed by Kaspersky Labs last January reported data loss due to staff members losing mobile devices. Though not as insidious as a rogue insider, Leaky Louise could potentially be more damaging -- especially if she works in a highly regulated industry, such as finance or health care.

How to keep them in check: A robust data loss prevention program that encrypts files at rest and on mobile devices is the most thorough way to prevent data spills, says Robert Hamilton, director of product marketing for Symantec's data loss prevention products. If a device is lost or stolen, encrypting the data on it will make it useless to anyone else. If an employee goes rogue or tries to take the data with them to another company, you can simply revoke their encryption keys so that they can no longer access the files.

"Aside from technical solutions, the best approach is employee education," he adds. "Most people don't realize what they're doing is wrong, or they think their employers don't care. When you do your annual security awareness training, you need to re-iterate that you do care."

IT frenemy No. 5: Slippery Sam
This software salesman has a license to fill -- and you're in his cross-hairs.

It seems like only yesterday you dropped seven figures on software licenses, but there's Sam on your doorstep looking to discuss renewals. When you tell him you're thinking about ditching your on-premises software for a cloud solution, though, the friendly smile fades. Maybe it's finally time for that compliance audit, he mutters darkly.

"The sales guy wants you to believe he's a partner in helping your organization succeed, but the relationship is usually more hostile," says technology attorney Rob Scott, managing partner of Scott & Scott, LLP. "The major software publishers have abandoned the strategy of partnering with customers and instead routinely investigate them for software license compliance."

Sam has a lot in common with his colleague, Hardware Hank. An old drinking buddy of Legacy Larry, Hank will happily extend the renewal on end-of-life equipment because he knows how much Larry hates change. He'll resell you gear he knows you can get much more cheaply direct from the manufacturer -- if only your procurement rules allowed you to do that -- at a 200 percent markup.

"Hank brings nothing to the table," says Howard. "He doesn't touch the product, provide warranty or services, or assist in the deployment. He makes a six-figure salary just by slapping his name on the sale."

How to keep them in check: If you encounter Hardware Hank, run as fast as you can in the opposite direction, suggests Howard.

"If you can't articulate the value a reseller brings, you need to find another reseller," he says.

The best way to deal with Slippery Sam is to secure a written agreement that forgives any past compliance transgressions, says Scott. The best time to do that is right before you sign the check. Then try to move core applications like email or Web hosting to the public cloud, where

compliance issues become someone else's headache.

IT frenemy No. 6: Cloudy Claudette
She has an Amazon Web Services account and she knows how to use it.

Claudette doesn't have time to wait for IT to give her what she needs. With one phone call and a corporate Amex card, she has entire server farms at her beck and call.

She's moving at the speed of business, spinning up Web services, and cranking out innovative ideas faster than you can say "IT asset management audit." But she's also creating IT sprawl in every direction -- as are her pals Darlene Dell, Ricky Rackspace, and VMware vCloud Vanesh.

More than half of IT pros surveyed by PMG, a business process automation vendor, say cloud sprawl is having a negative impact on their operations and budgets. Four out of five worry about security of data in the cloud, and nearly 60 percent are concerned about compliance.

"To me, the biggest concern is security," said Joe LeCompte, principal at PMG. "With cloud sprawl there's nothing to keep employees from putting sensitive files on Dropbox, forgetting they're there, and giving access to their files to people outside the organization. IT wouldn't even know about it."

How to keep them in check: If you can't keep your employees from using public cloud services -- odds are you can't -- IT's best tactic is to get there ahead of them and offer the same things as part of a managed services catalog, says LeCompte.

"If I can call up Amazon and get a server spun up in five minutes, why is IT telling me it's going to take two months?" he says. "The solution is for IT to act more like the Dropbox and Amazons of the world and get fast and efficient. Either it's going to happen in a way you can manage and drive, or it's going to happen outside your control -- and you have an even bigger problem."

IT frenemy No. 7: HR Harriet
Finding and hiring tech talent is hard -- and Harriet makes it even tougher.

On paper, your goals look perfectly in sync. You and Harriet both want to find and recruit talent into the organization, evaluate candidates, and make the right hires. But wait, Harriet has more paper for you to fill out. And still more after that.

That job you needed to fill three weeks ago will take another three months before it's approved and posted. The final job description looks nothing like the one you wrote. Meanwhile, you're doing the work of three people.

"Getting qualified people is hard enough, but human resources and IT never seem to mix well," says Mike Meikle, CEO of the Hawkthorne Group, a boutique management and technology consulting firm. "Getting your job requirements through the HR résumé SEO machine is nearly impossible. Suddenly it's a mishmash of bureaucratic phrases and meaningless buzzwords like 'empowerment.' And that midlevel programmer you want to hire now needs a Master's in Information Systems and 30 years of Java experience."

How to keep them in check: Eventually, every new hire will have to go through Harriet. The key is to keep her out of recruiting and evaluating applicants for as long as humanly possible, says Meikle.

"Try to find a way to work with potential candidates without putting HR in the middle," he says. "Harriet should only be involved in the nuts and bolts of the on-boarding process, not determining who's best suited for a position. That's your job."

IT frenemy No. 8: Frightened Frank
When "CSO" rhymes with "just say no."

Want to deploy 4G iPads to your road warriors? Need to spin up a new production server for the marketing department? Hoping to set up a Dropbox account so that you can access work files from your home? Ask Frightened Frank, and the answer to all of these questions -- as well as any others you might think to ask -- is no.

The result, of course, is an explosion in the number of BYOD Betties and Cloudy Claudettes, not to mention the security, support, and management problems associated with each.

A lot of IT managers -- especially those with the word "security" in their job titles -- are programmed to say no, says SafeNet's Gonen.

"They're not bad people," he says. "They literally think it's their job to say no. But the business has totally moved to yes, and IT needs to get there too."

How to keep them in check: The key to avoiding Frightened Frank -- or acting like him -- is to adopt a new mind-set, says Gonen.

Organizations need to accept that data breaches are inevitable, as well as put in processes and procedures to minimize the impact on their most sensitive data, he says. They need to find out what cloud services employees are using and set up simple policies on how to enable them securely.

"If someone comes to you and asks, 'Is it OK if we use Amazon Web Services?' you need to say, 'That's fine, so long as you use it in the following way,'" Gonen says. "The same goes with smartphones or Dropbox. Because even if you don't allow them, people will use them anyway. You have to give people a way to take shadow IT and make it real IT."

Related articles at InfoWorld.com:

- Read the Off the Record blog for on-the-job stories from IT pros -- and share your own
- 20 IT gotchas: How to avoid these common big blunders
- 12 "best practices" IT should avoid at all costs
- 8 biggest myths about managing geeks
- IT inferno: The nine circles of IT hell
- 10 hard truths IT must learn to accept
- 12 effective habits of indispensible IT pros
- The 9 most endangered species of IT
- IT personality types: 8 profiles in geekdom
- Dirty IT jobs: Grime and punishment
- Stupid user tricks 6: IT idiocy loves company
- A-Teams of IT: How to build your crack strike force
- IT turf wars: The most common feuds in tech
- IT admins gone wild: 5 rogues to watch out for

This story, "Eight is enough! IT's biggest frenemies," was originally published at InfoWorld.com. Follow the latest developments in IT careers at InfoWorld.com. For the latest business technology news, follow InfoWorld.com on Twitter.

IT Management