

The Challenge of Young Employees and Technology

According to a recent Cisco [survey](#), one in three college students and young professionals consider the Internet to be as important as air, water, food and shelter. Two out of three would choose having an internet connection over having a car! So it's not surprising that 70% of young professionals in the US admitted to breaking their employers' IT policies, with 2 out of three breaking policy most or all the time!

This is dangerous for government employers for a multitude of reasons, and not just data security and claim exposure. Who wants to face their board/commission/council/tax payers the day after the front page or TV sweeps week story on the web surfing habits of your employees!

Some tips on how you can address these issues (courtesy of legalloudspeaker.com):

- Your employees need to know the rules if you want them to be followed. Post them in the break room and ask them to sign a copy. Maybe do this every six months. Better yet, customize the windows log-in screen to be an acknowledgment that the user has read and will comply with the IT policy.
- You need to train your employees not only on what the rules say but also why they are important. Your young employees are just that – young. They haven't experienced a lot of workplace trauma yet, so they don't really understand (or fully understand) why management is so particular on sometimes very ambiguous things (I'm allowed to access LinkedIn but not Facebook – why?). Accordingly, at the same time you teach them the penalties for rule breaking: verbal warning, write-up, suspension, termination, you need to explain what happens to your entity when they break the rules. Translate that to what it means for their future. A lot of employees, not just young professionals, don't understand how much information about their use of technology is kept by IT, and that it is just a public records request away from being made public. Explain to them how government works, why the rules are in place and why they're not necessarily management's preference but are nonetheless management imperatives.
- We all operate off incentives and disincentives, so you can't expect someone to change their behavior if there's no incentive to do so. Reward those who abide by the rules and punish those who don't.
- Remove the opportunity and turn off the magnet that draws them to rule-breaking. Setup workplace-specific security settings that prevent garbage from ever entering your

building. Don't want Pandora, Facebook, or LimeWire? Turn them off. You have this power.

- Over 60% of young employees in the survey said it was the IT department's responsibility to protect information and devices. This is telling – they'll do what they can get away with. Accordingly, your IT department needs to be a proactive one that prevents the problem instead of responding to it. This isn't just a catch phrase. It costs less money to prevent a fire than to put it out and repair the water and smoke damage. The IT department needs to understand what young employees want to get at, what they should and shouldn't be able to get at, and how to prevent access to those things from inside your walls.

The finding of this [survey](#) impact more than IT policy. Anyone hiring or supervising young professionals should read and understand its implications for recruitment, motivation and supervision.