Tech Tracking
Rules of the game for a wired workforce
By Lisa Baker

Game on.

It’s 4:55 p.m., five minutes to COB, and if you’ve got your radio tuned to Mark and Dave on 1190 KEX, it’s time for the daily work-waster — the part of the show where the hosts unveil the newest avenue to dribble away the last few minutes of the work day playing games on the computer while appearing to be a dedicated employee.

Tip: Mute your speakers. Game sounds are a dead giveaway. Also, try not to yell “Woo hoo!” when you reach level four.

According to game developer PopCap Games, based in Seattle, one-quarter of office workers and two-thirds of CEOs regularly play online games at work.

In the company’s survey, respondents said they played games to relieve stress. Game makers say online games can refocus the mind and actually increase productivity. Sort of like naps.

Be that as it may, non-work Internet use in the workplace is extremely common, and it’s not just the gaming sites getting the action. Car shopping, house shopping, Christmas shopping, YouTube watching, chatting, blogging, reservation-making, car-renting, and bill-paying top the list of common online workplace activities.

Then, there are the most troublesome ones: online gambling and online porn.

Companies are fighting the battle a number of ways and for a number of reasons. For some businesses, time and bandwidth waste is the biggest concern, as cubicle-bound workers suck up company capacity watching streaming content while deadlines loom large.

Managing email — a usually legitimate work activity — has become such a productivity killer that “life hack” sites now offer 12-step programs to cure email overload and, for those who become overly fascinated with it, email addiction.

There are no reliable figures on how workplace Internet affects the bottom line, but local businesses big and small say loss of productivity is only one of a nest of problems that can crop up. Among them: social diseases that infect the network.

Gaming sites and download sites are often associated with “malware,” or malicious software that board your computer during an innocent game and then spread across your company’s network, destroying data files and hamstringing hardware.

Some data loss is survivable, and hardware can be repaired or replaced. Something that can't so easily be resurrected? Company reputation.

It's among one of the more serious dangers lurking on the Web.

Social networking sites are full of workers anonymously gossiping about their companies — and bosses — in unflattering ways, posing for revealing photos, spilling company secrets, or flaming complaining customers.

Online gambling habits lead to embezzlement.

Online porn habits lead to sexual harassment lawsuits.

It's a jungle out there.

High stakes game

It's such a problem that a new industry has grown up to address it. Reputation repair companies monitor the Internet for inflammatory or strategically injurious posts — like the release of new product details or company plans — and work with companies on damage control.

How high are the stakes? The negative postings of a single disgruntled employee armed with a blog can outrank a company's own web page and show up at the top of the list of search engine results.

Private companies are not the only ones needing scythes and pith helmets to hack through the underbrush. Government, too, is finding the tech revolution challenging.

Last year in Ohio, a police officer's MySpace page featured pictures of drug-bust evidence and a cruiser's speedometer at 100 mph. The officer? Fired.

A year ago in Arlington, Ore., the newly-elected mayor was recalled after photos of her posing on a fire truck in lingerie were found on her MySpace page.

Teachers posting inappropriate comments on social networking sites and including their students as "friends" on their sites have prompted statements from teachers' unions strongly discouraging any use of MySpace or Facebook.

Catherine Paglin, writing for the Oregon Education Association, the state's teacher's union, advised in an article in April 2007 that teachers avoid such sites, citing disciplinary actions taken against teachers all over the country who spilled about their, um, personal habits on social networking sites.

Indeed. In Phoenix, a television news report found questionable MySpace pages posted by a number of local school teachers — pages that included profanity and inappropriate photos.

Paglin warned Oregon teachers that “friends” who post inappropriate personal messages to a teacher’s personal site can destroy that teacher’s reputation. “Even if you go to the trouble of screening all your friends’ comments before allowing them to be posted, a visitor to your profile can follow the links to your friends’ sites and might find information about you there that you would rather keep private, such as photos or videos taken at a party or during a night on the town,” she wrote.

An additional danger, she said, is casual social interaction with students on the web, which can become inappropriate quickly.

The stakes are especially high for public sector workers, whose workplace emails, blogs and even phone records are public record.

Trust and verify

The online behavior of employees is a new area in human resources, but the toolbox is growing by leaps and bounds each day. Companies agree that the first and most important tool in the box is education: Workers have to know what’s allowed, what isn’t, and what will happen if they violate policy, whether they’re blogging at home or playing games on the work clock.

Most companies with internal computer networks have tools to monitor their workers’ email and Internet use, and can easily summon a list of sites visited online. Even erased messages can be reconstituted.

Amy Angel, an attorney with Barran Liebman, a Portland law firm that specializes in labor law, said courts have held that employees using their company network and equipment can have no expectation of privacy in their use of that equipment. At the same time, she says companies must have clear policies that inform employees that their online activities can be accessed by the boss at any time.

Some companies prevent problems by installing filters that prevent network computers from accessing certain sites or from downloading certain kinds of files — either because they consume too much bandwidth, they might be inappropriate, or they may contain malware. Some companies have programs that prevent certain emails from reaching their intended targets.

But given the steady stream of conversation, video and audio passing through servers each day, such measures are often not enough. That’s where monitoring comes in — and many companies get queasy about eavesdropping on their employees.

In general, says Judy Clark, a consultant with HR Answers in Tualatin, it’s good that employers pause before doing something particularly invasive — for two reasons. One is practical: Tracking and monitoring are time-consuming activities few businesses can afford to engage in unless there’s a demonstrated problem with a particular employee. “It’s just not realistic that employers can spend an inordinate amount of time wandering around employees' Google searches and emails. They ought to have better things to do." The other issue is employee retention: "I just don't know a lot of employees who respond well to Big Brother."

Clark says that while it's possible for companies to ban all non-work use of the Internet while on the job, it's not practical and most workers view it as unfair. "There is such a blurring of what's employment and what's personal time these days," she says. "BlackBerrys, smartphones … People log-on to their email at night and stay up with it and respond while they are on their personal time. And, that's probably only a quarter of the way it will be in the future. It's hard to advise a client to be really hard-nosed with heavy monitoring of every activity when they benefit from this greater amount of productivity. When your employee is plugged-in 24/7, well, that calls for new thinking."

And so, Clark says, if an otherwise productive worker chooses to make a reservation for dinner online, or text her children to make sure they're home from school, a boss would be well advised to leave it alone. Another good position, for those employees who want to shop online in extended fashion, is to tell them they can use the company network for personal use when they're off-clock — either before work, after work or on breaks, Clark says.

Some public sector organizations have exceedingly strict policies that Clark says have led to workers being fired simply for making reservations for professional conferences with office equipment. Draconian policies make it difficult to retain employees, who like to feel that there is some level of trust in the workplace, she says.

"If you go to the other end of spectrum, there are those who haven't got a clue how much time their workers spend in individual pursuits, like fantasy football or holiday shopping, or whether they're posting pictures to MySpace or Facebook. And they have no idea whether the level of productivity they're getting is appropriate or diminished."

Cops gone wild

Productivity is the least of the potential problems when cops run wild on the Internet. Brian Schmautz, spokesman for the Portland Police Bureau, says young, techie cops have to be taught about what can and can't be said — and photographed — for Internet sites. "Occasionally you have young officers who are more Twitter, Facebook, MySpace kinds of people who have posted things about an investigation and we've had to squash it," he says. "We remind officers that there are a number of orders, from showing pictures of evidence — you can't show crime scene evidence — to talking about criminal investigations unless the case is adjudicated. What's public record is public record for cops also," Schmautz says. "If someone confesses a crime to me tonight, I can't go home and blog about it. It would be prejudicial."

Schmautz says the problem is a generational one. "People of my generation say, 'Why would anyone want to blog?' We don't understand the point of blogging in life, but for this next generation, it's their way of processing their lives. And now everyone carries a personal cell phone while working, so let’s say they take a picture while they’re working and then show it to people in a bar, ‘Hey, look at this!’”

The bureau does not attempt to look for its officers in social networking sites or anywhere else because, Schmautz says, tracking the online activities of 100 officers would be impossible. “We do have to monitor the dispatch system because if an officer says, ‘Well, that guy was a jerk, and I told him off,’ a defense attorney can use that. Even if an officer texts another officer something — that’s all discoverable.”

One thing the department does do: It searches networking sites as part of background checks for applicants. “I’m amazed at how many people who want to get involved in law enforcement are on these sites and fail the background check because they [post] about drug use and personal life choices that are not consistent with being an officer.”

When play is part of the job

Curt McKay, senior project manager for Quango, a 20-employee, Portland-based design and marketing firm, remembers the day the Line Rider game arrived at the office after making the rounds on the Internet. This is the game where you draw a hill with your mouse, then hit a button to watch the scarf-wearing sledder attempt your hill and, inevitably, crack up and lose the sled altogether.

Don’t ask us how we know this.

Far from filtering it out or restricting employees from playing games like this one during work hours, McKay said the company encourages them to find out what makes it tick and why it’s so popular.

“Someone developed this application and it found its way around the world. And so we studied it … How easy is it to make? What can we learn from it marketing-wise? It was super valuable to us. It’s that kind of information that plays a part in how we help someone advertise or market something,” McKay said. “Preventing employees from playing it would hamper that.”

Quango’s overall policy is to look at results before clamping down on employee behavior. “If you’re performing, we think you’re an adult and you can do what you want with your time. If you’re looking up personal email or shopping for a car, it’s okay as long as work’s getting done. It helps to take a break. I’ve found personally that it’s nice to be able to do some online shopping while I’m at work. It’s a better work-life balance. I probably do some work stuff at home, too. The thing is, I’m a big boy and I can handle responsibility.”

Because part of the company’s mission involves, as McKay puts it, “acquiring stuff” from vendors or clients, blocking downloads would be a practical nightmare. By the same token, client materials are under virtual lock and key to ensure that only authorized personnel have access.

For an extreme version of lock and key, there's Mentor Graphics, the Wilsonville-based high-tech company. Ry Schwark, spokesman for the company, says there's little policing of employees' personal business on the Internet and that "obviously, there may be some of the work wasting going on, but on the whole, we're trusting employees to get the job done. So, they can check sports scores near the end of the day; we don't care. We're not going to be Big Brother."

That doesn't mean the company's security is lax. Because intellectual property is precious in the high-tech business, the company's legal arm continuously reminds its workers how precious it is and how important it is safeguard it. An online training program, company officials say, is the first line of defense that prevents employees from spilling important beans.

But there are other protections.

The company employs security measures in every laptop and desktop that blocks employees from downloading potentially dangerous applications. Firewalls prevent hacker programs from gaining access through any virtual door left unlocked by careless workers.

Ananthan Thandri, chief information officer with the company, says "hacking happens to every company, all the time. That's what the firewalls are for, and we have them all over the world and monitor them from here in Wilsonville."

Even so, he says, "hackers are always a step ahead of us. We're always having to catch up."

Nike officials would not comment to *BrainstormNW* about workplace Internet use, but an employee blog mildly critical of the way some company officials spend cash briefly went public in 2006 under the name Swooshblog. The writer was astounded at one point that one of his fellow employees had leaked internal information to an *Oregonian* reporter — something he blogged that he would never do.

The blog ended when the writer conceded he was bored with the job — the blogging job, that is. "There just isn't that much to write about … " he wrote.

"I'll go back to work and be the guy that sits next to you," he wrote in his farewell post. "The guy you ride the elevator with, the guy on the treadmill next to you, or even the guy that signs your checks."

Employees unplugged

Blab, er, blog all you want.

It was likely the most enticing thing a high-tech company could tell its employees, especially one as tightly held and message-controlled as Beaverton-based Intel.

But there was a plan behind the company’s invitation — a plan to join the bloggers and social networkers, because silencing them was clearly impossible.

The idea: to use blogging as a way to connect with customers, create relationships, increase brand loyalty and … fight negative postings and reputation-destroying buzz with positive spin of their own. The method had the added advantage of providing a channel for employees to contribute in ways that might discourage them from starting anonymous — and anonymously damaging — insider posts someplace else.

Sort of like telling your kid he can have a beer as long as he drinks it right here in front of you.

Reputation repair companies say starting blogs of your own creates a sea of positive pages that will counter — and likely drown out — naysayer pages when search engines kick out results with your company name attached.

But like any other major corporate move, it wasn’t a simple one. It meant creating a whole new arm of Intel, called the Social Media Center for Excellence, to ensure that the venture wouldn’t result in a free-for-all in the public domain.

Employees are drilled on the rules of engagement, the first of which is to understand that they can’t separate their comments from Intel and say they’re not representing the company. “They need to understand if they blog things related to their job, they will be seen as spokespeople for the company whether they are or not,” says Kelly Feller, social media strategist for Intel. Other rules? Be respectful, be honest, and don’t release private company information — a biggie.

Feller says the company hopes the participation of Intel staff in the blogosphere will have a “viral marketing effect” that will create excitement about the company.

Other companies, including Nike and Microsoft, have started their own efforts to rock the blogspots, but Intel’s venture is the most public foray of the three: Its staff released a statement announcing the new policy and asking for feedback.

Feller insists that employee posts are not previewed or pre-screened, making the blogs more authentic, but also risky. “Is there inherent risk in doing this? Yes. But we’ve realized that all of these online conversations are already happening, and it does no good to stand on the periphery and not participate.”

Another advantage of the strategy, from a company point of view?

With company staff engaged in blogs and networking sites everywhere, at work and at home, the company will have eyes — and ears — everywhere.

So, if you have an itch to, well, comment about Intel, don’t be surprised if the next voice you hear or read is from inside Intel.

Talk about them and they will know.

***BrainstormNW* February 2009**