SpectorSoft

Mitigating the Top 5 Threats to Your Business

1.888.598.2788 | www.spectorsoft.com

Mitigating the Top 5 Threats to Your Business

Most business leaders know to focus on certain specific threats to their business. You keep an eye on overhead costs, for example, so that they don't eat up your profit margin. You think about disasters, and how your business might survive during a power outage or a major event like a flood. You make sure you've got all the right liability and worker's compensation insurance. You hire a pest control firm to deal with insects, and a plumber to keep the water flowing in the restrooms.

But most businesses completely overlook five of the biggest threats to productivity, to stability, and to legality. Overlooking these threats can – even in a small business – cost upwards of half a million dollars a year. Not dealing with these threats can land you in court – with all of the costs that implies. Ignoring these threats can wipe out your competitive advantages and literally hand your most important business assets to your competition.

These threats all stem from one source: your employees. Half the time, they're not even creating these threats maliciously – they just don't stop to think about what they're doing.

When your employees think that they're acting anonymously, and that their actions have no personal consequences, they're liable to do anything – including finding a way around your filtering software.

Threat 1: Harassment Lawsuits

Not everyone thinks that every joke is funny, and when "borderline" humor starts making its way through your company's email and instant messaging systems, *you* become the butt of the joke. When jokes contain racial slurs, sexual humor, or other inappropriate content, it's your duty to put a stop to it *immediately,* and to provide appropriate discipline and sensitivity training to the perpetrators. Failure to act swiftly and appropriate can make *you* and your business just as liable as the jokesters.

The same applies to employees who visit an inappropriate website. Sure, just looking at a website doesn't harm anyone – until someone *else* catches a glimpse over the offending employee's shoulder.

Most companies try to address this problem via filtering software. The problem is that inappropriate comments and websites spring up and evolve faster than filtering software can keep up. When your employees think that they're acting anonymously, and that their actions have no personal consequences, they're liable to do anything – including finding a way around your filtering software. And when they find a way, and inevitably offend someone else's sensibilities, it isn't your filtering software that ends up on the chopping block. It's you, and your business.

Threat 2: Loss of Information

In today's competitive marketplace, *every* piece of information is critical. Your employees, of course, have access to a great deal of confidential information. They're excited about what they do for a living, and they're excited about what the company is about to do. Sometimes they just can't resist sharing a little – perhaps "leaking" a rumor onto an Internet message board about an upcoming product launch, or providing just a bit too much detail when sending an email, or

confessing insider information over a chat message. Sometimes it isn't the information itself that's a problem, but the *timing*, such as employees who discuss upcoming product and service plans during legally mandated "quiet periods."

In the end, of course, you're the one who pays the price. Once the information is out there, it's *out there,* and you'll spend an infinite amount of time trying to track down who was responsible. That's especially true when employees use Internet-email accounts. You simply don't have an audit trail for those activities, making it incredibly difficult to track down the perpetrator and deal with the problem.

Once again, many breaches of this kind aren't intentionally malicious – your employees just aren't always armed with good decision-making skills, they get a little overexcited, and they let slip something that they shouldn't have.

Threat 3: Wasted Time

It's the easy access, and the lack of personal consequences, that makes employees simply "not think" when they're wasting time…

Let's say your average employee makes $60,000 per year. They sit in front of a computer for most of the day, and quite frankly they get a little bored. A little Facebook time here, a few minutes playing games there, and before long – on average – they've wasted an hour of the day. That's just seven minutes out of every hour – who can they be hurting with such a brief diversion? They're hurting you, and your business, to the tune of more than $7,000 per year in lost time. If you've got just 50 employees, you're probably burning more than a quarter million dollars a year keeping them amused and entertained.

Now, none of your employees *means* to do it. Everyone expects to get a little brain-break now and again. But non-work surfing on the Internet is a little different from an hourly trip to the water cooler, because the Internet makes it easy to get carried away. You start catching up on Myspace, and before long it's not a 5-minute brain-break, it's an *hour* wasted out of the day. 250 hours a year. 12,500 hours a year across 50 employees. It's insane.

It's the easy access, and the lack of personal consequences, that makes employees simply "not think" when they're wasting time like this. And even if you decide you don't care about an hour waster per day, there are definitely employees who'll take advantage of that largesse, and take you for *hours* per day – often wasting more time than they spend actually working.

Businesses again turn to filtering software to help, with the idea of banning access to "time wasting" websites. Good luck. Some of those "time wasters" are actually legitimate for *some* employees, like the ones responsible for updating the *company's* Facebook page or Twitter feed. And the number of time-wasting sites *will* grow faster than your filtering software's ability to keep up. So in addition to the wasted productivity – which will still occur – you'll start wasting *more* time trying to manage your filtering system.

Threat 4: Inappropriate Downloads

The Internet, it sometimes seems, was born to make things difficult on businesses. If employees aren't wasting time surfing the latest Flash game website, they're downloading illegal music, illegal videos, virus-infected

executables, and who knows what else. Yes, you can implement virus scanners and file blockers, but there's an entire cottage industry dedicated to letting your employees bypass those protections.

It's the same mentality already covered: your employees aren't acting with deliberate malicious intent, they just *want* that ringtone or "elf bowling" game so badly, and there's no personal consequence in them having it, so they find a way to get it.

One virus-infected game on your network and you'll spend thousands of man-hours repairing the damage. One collection of illegal MP3 or video files and you'll spend countless man-hours defending yourself in court, and thousands of dollars in fines. Don't you wish your employees could just *think* for a moment before they clicked "download?"

Threat 5: Wasted Effort

This is one of the most subtle threats of all, because your employees *truly* don't even know they're hurting you. This is the time that's wasted because your employees aren't trained to be as productive as they could be. Perhaps they're wasting time formatting a Word document, not realizing that there's a built-in template to do it for them. Or they're struggling to operate a line-of-business application, without realizing that your developers built in a shortcut five versions back. Or it's your help desk, desperately trying to solve a user's technical problem, running around in circles because they can't duplicate the problem and the user can't describe how *they're* causing the problem.

Seems like there's nothing you can do about this threat, and in fact most businesses just tend to throw up their hands and accept it as the "cost of doing business." Pity. In this day and age, even minor productivity gains can make an enormous difference. Employees already feel overworked and under-appreciated; if you could help them do their work with a bit less *work,* they'd certainly feel better about it.

The Fix: A DVR For Your Employees

The first four threats discussed above have a common theme: Your employees wouldn't engage in those activities if they thought there were personal consequences for doing so. In other words, if you could hire someone to stand and watch over their shoulders, all day, they wouldn't surf those websites. They wouldn't waste their time. They wouldn't download those files.

Of course, you're not going to hire people just to stand and watch other people. But you *can* implement *User Activity Monitoring* (UAM) software. Typically deployed as a small client application on your Windows and Mac computers, UAM software literally records your employees' actions, including keystrokes and potentially even including screen snapshots every so often. Malicious websites? Contextually blocked, and also logged so that you know about the attempt. Time-wasting sites? Logged. Inappropriate email messages? Logged. Rumors spread via Instant Messenger? Logged.

Typically deployed as a small client application on your Windows and Mac computers, UAM software literally records your employees' actions, including keystrokes and potentially even including screen snapshots every so often.

With that information logged to a central data store, the UAM software can generate reports. You'll see the average amount of time spent on Facebook – and be able to drill down to the employees who are at the top end of that average. You'll see who's posting confidential information, and where they're doing it, and even get real-time alerts when it happens.

You'll also be able to mitigate threat number 5, by having training and productivity specialists review employees as they're working. You'll *see* when they're working harder than they need to, and be able to build training plans that better equip your employees to do their jobs. Your employees will appreciate you making that investment in them, and they'll enjoy a better quality of life simply because they'll work more efficiently, with less wasted effort.

UAM software can do all of this, and more. By letting your employees know that their activities in the workplace *do* matter and *are* being monitored, they'll *think* before engaging in reckless activity. Knowing that personal consequences are possible, you'll generally avoid the problems in the first place, simply because your employees will make better decisions. Then you'll be able to help them work more efficiently and effectively. It's a better way to run a business, and a better way to maintain relations with your employees.

By letting your employees know that their activities in the workplace do *matter and* are *being monitored, they'll* think *before engaging in reckless activity.*