

Millennial Meltdown

Balancing Innovation with Productivity and Security

While tools such as Web 2.0 applications, IM, P2P and portable USB media can be great for business innovation and productivity, they're often dreadful for IT security. The first instinct of many businesses is to simply ban the use of such technology. This may eliminate the danger, but it cuts off innovation at the knees. In order to truly get ahead, organizations must find a way to strike a happy balance that allows for the safe use of new technologies.

Introduction

When a company is in a rut, sometimes the young worker can be the perfect medicine to cure what ails. Bright-eyed and fresh, the youthful millennial is computer savvy, full to the brim with ideas about how to leverage new technologies, and excited to get to work.

Such a prospect is a dream for businesses, especially as the economy tightens. Indeed, any group of employees that can use technology to improve productivity and stimulate innovation on the cheap is a valuable demographic. In this environment, the ability to dream up new products, campaigns and ways of engaging with the customer through Web 2.0 applications, or to transfer information quickly and easily via IM or portable USB media or even peer-to-peer networking, can be a great advantage.

And, while many of these tools can be great for business innovation and productivity, they're often dreadful for IT security. Unfortunately, though, the first instinct of many businesses is to simply ban the use of technology such as removable media and [Web 2.0 applications](#). This may eliminate the danger, but it cuts off innovation at the knees. In order to truly get ahead, organizations must find a way to strike a happy balance that allows for the safe use of new technologies.

By educating employees about the risks, setting policies and implementing ways to monitor and enforce those policies, organizations will reap bene-

fits their competitors may well be giving up through wholesale bans on new technology. The workforce will not only be more productive and innovative, they'll also remain happier and more loyal to the company cause. Enforcing flexible policies will get greater buy-in and fewer people will make it their mission to get around policies.

“If IT is seen as the force inhibiting progress, users will find paths around them. We try and make our policies flexible enough to accommodate the fact that end users will at times bring in outside technology or programs in order to make their job more productive. We encourage these staff to talk to us and let us see how it could fit in the organization or what other technologies we may already have that they may not be aware of.”

Rob Israel, CIO

John C. Lincoln Health Network

Doing so may even help reduce costs. After all, a personal, [secured USB device](#) costs nothing to an organization, and the proliferation of these devices very well may take a bite out of hardware purchases—a trend that Gartner calls the ‘consumerization of IT.’¹

1. www.gartner.com/press_releases/asset_138285_11.html

Employee 2.0

Perhaps the most accurate truth about the newest generation of workers is their inextricable relationship with Web 2.0. Workers in their 20s and 30s have grown used to broadcasting news and 'marketing' their lives to friends and associates over MySpace and Facebook. They regularly exchange documents over Web mail, IM or Google Office accounts, and many of them started harnessing the power of the blog and community-based content years ago, simply in the name of fun and connecting online.

And now many of these employees expect to continue to use these tools in the name of productivity or even just amusement during downtime.

“...the security challenges of Web 2.0 applications are both technical and commercial in nature.”

Fran Howarth, Analyst, Quocirca

According to a poll recently conducted by Applied Research-West, approximately two-thirds of millennial workers said they regularly access their Facebook and MySpace accounts at work, compared to 13 percent of older workers. And while only 54 percent of older employees access Web mail accounts at work, more than 75 percent of millennials do the same.²

Unfortunately, those who could be categorized as 'Employee 2.0' aren't aware of the dangers posed

by certain websites and [Web 2.0 applications](#), and insist on using them even when employer policies ban them. In fact, the experts with the consultancy Accenture found in a poll among this cross-section of young employees that more than half either didn't know about or didn't follow company IT policies. In one instance the company reported that when it questioned college age up to 27-year-old employees, 31 percent said they didn't know if their employers had policies for posting company information online and 40 percent admitted knowing that that their company had policies but the workers chose to ignore them anyway.

This is extremely troubling when considering the fact that rich media Web 2.0 is one of the most threatening emerging risks on CSO's radars in 2009, according to Baseline Magazine.³

Fran Howarth, an analyst with the firm Quocirca, nailed the problem on the head, explaining that the issue with Web 2.0 applications is that they are not only more vulnerable than most applications but also make it easier to share sensitive information. "On the one hand, the underlying technologies used actually raise the risk of web-based attacks whilst, on the other, the way that users interact with Web 2.0 applications increases the risk that sensitive information will be misappropriated," she wrote. "This means that the security challenges of Web 2.0 applications are both technical and commercial in nature."⁴

2. www.networkworld.com/news/2008/032008-millennial-web-20-security-challenges.html?fsrc=netflash-rss

3. www.baselinemag.com/c/a/Security/Top-10-2009-Security-Threats-and-Vulnerabilities/

4. www.it-analysis.com/content.php?cid=10162

As a recent article in the Wall Street Journal points out, social networking sites such as Facebook, Twitter and LinkedIn lull users into a sense of security while providing hackers a platform to carry out phishing and malware attacks.

Me, Myself and My iPod

This next generation of leaders is also more gadget savvy than any other generation of workers. This 'iPod generation' has practically never known what it's like to live without a USB stick in their pocket and a set of headphones in their ears. According to a survey of millennials conducted by PriceWaterhouseCoopers, over 86 percent own an iPod or mp3 player.

Over 86 percent of people own an iPod or mp3 player.

PriceWaterhouseCoopers

It is second nature for these employees to use USB storage devices, mp3 players and tricked out iPods while working. But as so many data breach reports have shown [unmanaged USB devices](#) are a major source of [data leaks](#) and worm outbreaks. Similarly, unmanaged iPhones and smartphones can pose serious dangers when considering the fact that users can install third-party applications at-will that could potentially hold malware just waiting to attack the network once the phone syncs into the network.

Sadly, many IT departments have taken a binary attitude about USB devices and the employees who use them. Either the department chooses to totally ignore personal devices on the network—taking the stance that it's the employee's device, so why bother supporting or even acknowledging its existence—or to completely ban devices altogether. Neither approach is good for the business.

Ignore USB devices and you'll ignore the possibility of data walking out the door or malware spreading through infected devices. Impose a draconian ban and you'll face resentment among young workers and their managers, who ultimately want to keep the talented youth movement happy and productive. Plus, banning these devices is almost an extended way of ignoring a problem. Adopting a '[disable ports](#) and forget' attitude can be costly if a system is overlooked, as now the department doesn't even have the USB problem on the radar and has no way to track rogue devices. This is exactly what happened at Countrywide Mortgage last year when an employee made off with hundreds of thousands of records on a USB device hooked into a non-disabled machine.

The Great Compromise

In its report on millennials in the workplace, Price-WaterhouseCoopers emphasized the importance of this generation to the future workforce and noted that, “We feel that this group will put more pressure on employers to have clear employer brand values against which they can be evaluated. We feel that if employers do not live up to employee expectations, millennials may be more likely to look elsewhere.”

Part of that pressure will be to offer a workplace that allows the use of gadgets, Web browsing and more in the workplace for not only business purposes, but also leisure use as these employees work long hours to drive profit to the business.

Often businesses forget how much a ban on technology or innovative practices can chafe at employees, particularly the dreamers, the innovators, the late-night workers who care most about an organization. They say, “All I want is what’s best for this organization and yet it can’t even let me use a simple [USB hard drive](#)? What’s wrong with them?”

Even though it may be an employers market, the very best employees are still in short supply. It is simply too costly to alienate these workers through stiff policies and a lack of regard. Because once loyalty is lost, it is hard to regain.

Clearly, the folks from HR and IT security are at odds. Fortunately, there is plenty of room for a successful compromise.

Rather than impose drastic bans on devices or Web 2.0 applications, businesses need to develop enforceable acceptable use policies that selectively prohibit certain activities, limit time on others and so on to limit the risk that it has prioritized.

For example, at [John C. Lincoln Health Network](#), Israel and his staff built a policy that was flexible enough to allow exceptions if staff members were able to individually justify the business case for specific tools:

Customer Case Study: John C. Lincoln Health Network

“We realize there might be a very good reason why you need a thumb drive or a CD burner and so on, so we encourage them to come talk to us and see what we can do. We say, ‘Let’s see if we can come up with a different alternative for you to connect, whether it is remote access with a VPN, so you don’t have to walk around with a thumb drive in your pocket. If there are existing technologies that can meet your needs let’s document why you need it for our security audits and work in conjunction with you so you can continue to do your job.’”

Then we wrote our policy around that, stating that we see peripheral devices and the ability to read/writes to removable media as a severe security threat with patient privacy and business confidentiality. Therefore, we have implemented the following policy and procedure and this is how it works. Users must fill out a form requesting access to x, y or z and define why they need it.”

Once a policy is written, IT has to find a way to automate monitoring and enforcement so that clueless or willful employees don't skirt the rules. Israel believes this is absolutely key, "You've got to make sure you have something to enforce the policy. Just putting a policy out there saying, 'You can't use thumb drives, it's a no- no' isn't going to work because you can't track it."

"You've got to make sure you have something to enforce the policy. Just putting a policy out there saying, 'You can't use thumb drives, it's a no- no' isn't going to work because you can't track it."

Rob Israel, CIO

John C. Lincoln Health Network

Have Your Cake AND Eat it Too

[Lumension® Data Protection](#) gives security professionals the tools needed to effectively embrace these productivity tools. Through device whitelisting and through flexible and granular policy enforcement, organizations can not only ensure millennials use only accepted devices, but also enforce certain times of use. That gives an organization the flexibility to allow some millennial leisure pursuits while preventing abuse of company time.

[Lumension® Endpoint Protection](#) employs [whitelisting](#) as well to enable only authorized applications and prevent rogue applications and malware from even getting a chance to run on corporate endpoints and servers—eliminating the risk that a well-meaning millennial will stumble onto a site with hidden malware that could compromise the whole network.

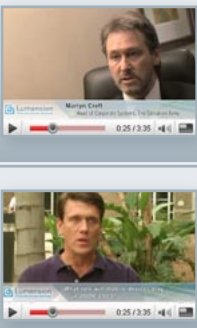
Lumension also gives IT powerful auditing and monitoring tools to keep track of user activity with accepted applications/files to ensure that employees are not accessing data they shouldn't be. IT can now prevent employees from absconding with certain types of data on their iPhone and thumb drives so that security managers needn't be scared every time an employee plugs in a USB device. And security managers now have access to effective reports which can be used to pinpoint certain millennial users who may need additional education about their risky activities.

About Lumension

Lumension, a global leader in operational endpoint security, develops, integrates and markets security software solutions that help businesses protect their vital information and manage critical risk across network and endpoint assets.

Lumension enables more than 5,100 customers worldwide to achieve optimal security and IT success by delivering a proven and award-winning solution portfolio that includes Vulnerability Management, Endpoint Protection, Data Protection, and Reporting and Compliance offerings. Lumension is known for providing world-class customer support and services 24x7, 365 days a year.

Headquartered in Scottsdale, Arizona, Lumension has operations worldwide, including Virginia, Florida, Luxembourg, the United Kingdom, Spain, Australia, India, Hong Kong and Singapore. Lumension: IT Secured. Success Optimized. More information can be found at www.preventia.co.uk



Video: Success Story
Salvation Army Protects the Integrity of Data and Global Brand

Video: Hot Topic
Mobile Devices in the Workplace: Striking the Right Balance

Whitepaper - New Insider Threat Emerges in the New Economy

Webcast - Protecting Company Information: Why, How and What If

Key Steps to Protecting Your Vital Information



Quantify your risk of unmanaged USB Devices

with *Lumension*® Device Scanner Pro

Webcast - Data on the Edge: Protecting Your Business with *Lumension*® Data Protection

Whitepaper - Taking Control of Your Data: Protecting Business Information from Loss or Theft

Protect Your Vital Information Today



Enforce USB Device and Application Usage Policies

with *Lumension*® Endpoint Security Suite

FREE