

5 Steps to Embrace the Consumerized Workforce: Finding Ways to Balance IT Risk and Productivity

While tools such as Web 2.0 applications, IM, P2P and portable USB media can be great for business innovation and productivity, they can introduce significant risks when not managed properly.

Unfortunately, too many organizations fall into two extremes when it comes to reining in these risks. On one end, very security-conscious organizations have reacted by simply banning these technologies — a practice quickly falling out of favor among line-of-business leaders. And on the other end of the spectrum, many more practical organizations have chosen to develop acceptable-use policies for these tools without any real enforcement. To truly realize the benefits while curtailing the risks, organizations must find a way to strike a happy balance that allows for the safe use of new technologies.

Introduction

Today's collaborative working environment has upped the ante for how productive employees go about their business. Organizations and managers see the value in workers' ability to dream up new products, campaigns and ways of engaging with customers through Web 2.0 applications and social media platforms. Colleagues expect their cohorts to keep up with work no matter where they are in the world, staying in touch via IM and text, toting information around on USB devices and smartphones, and trading documents via e-mail or even peer-to-peer networking. As long as the job gets done, most line-of-business managers are happy.



And while many of these tools can be great for innovation and productivity, their very nature introduces an inordinate amount of risk to organizations — be they in the public or private sector. Most of these new devices and applications are designed to maximize connectivity and collaborative sharing of data — a big boon for workers, but a potential minefield for security and privacy advocates.

While it would be easy to simply ban the use of technology, such as removable media and Web 2.0 applications, practicality makes this prospect impossible in today's world. Technology bans may eliminate the danger, but they also cut off innovation at the knees and chafe at some of the most important employees within the organization: the dreamers, the innovators and the late-night workers who care most about their work.

By educating employees about the risks, setting policies and implementing ways to monitor and enforce those policies, organizations will reap benefits 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 organizational cause. Enforcing flexible policies will get greater buy-in, and fewer people will make it their mission to get around restrictive policies.

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. Likewise, Web 2.0 applications provide a cost effective and easy way to communicate with customers, partners and vendors — and they definitely offer competitive differentiation advantages when done right.

Employee 2.0

The stunning growth in Web 2.0 and social media activity has taken the workplace by storm over the last several years. According to the most recent figures, 94 percent of enterprises have users who utilize social networking sites¹ — often mingling business with pleasure, communicating with friends and associates through Facebook, LinkedIn, Twitter and more. And approximately 62 percent of users say they check social networking sites at least once per workday².

Unfortunately, most employees — particularly the younger ones most likely to use social media and other Web 2.0 applications — aren't aware of the dangers posed by certain websites and Web 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.

The company reported that when it questioned employees from college age up to 27 years old, 31 percent said they didn't know if their employers had policies for posting company information online, and 40 percent admitted knowing that their company had policies but they 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 CSOs' radars today, according to Baseline Magazine.³ And it's no wonder why — industry experts estimate that 78 percent of Web 2.0 applications today propagate malware.⁴



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

Fran Howarth – Analyst, Quocirca

1. Palo Alto, The Application Usage and Risk Report, Spring 2010
2. Symantec, Social Networking at Work Survey, June 2010
3. Baseline Magazine, Ericka Chickowski, “Top 10 2009 Security Threats and Vulnerabilities,” 2009
4. CA, Inc., State of the Internet 2009
5. Quocirca, “Web 2.0: next generation web threats,” 2008



Weighing The Pros And Cons Of Web 2.0

32 percent of employees said they would factor in a ban on accessing social networks from the workplace into a decision on whether or not to work for a company⁶

- » 82 percent of IT security administrators say social networking and other Web applications lower the security posture of their organization⁷

In its report on millennials in the workplace, Price-WaterhouseCoopers emphasized the importance of this generation to the future workforce and noted, “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.

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.



Me, Myself and My iPhone

Meanwhile, as the growth in social media and Web applications continues to mushroom, so too do the number of gadgets that employees use to access new websites and applications. Today’s typical employee comes to work armed with one or more devices such as smartphones, storage devices and mp3 players.



But 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 toward 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.

6. Symantec, Social Networking at Work Survey, June 2010

7. Ponemon Research, Web 2.0 Security in the Workplace, August 2010

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 talented millennials 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 in 2008 when an employee made off with hundreds of thousands of records on a USB device hooked into a non-disabled machine.



- » 76 percent of security and IT leaders believe user influence on decisions to acquire devices and applications is increasing
- » The majority of IT leaders say their companies have policies regarding connection of personal devices on the network, but almost 60 percent reported unauthorized connections still occur
- » 23 percent of organizations have experienced a serious security incident or breach due to the connection of a personal device on the network



Source: RSA, CIO Marketpulse, July 2010

Taking Action

To strike the right balance between productivity and security, organizations need to take a defense in depth strategy. The following five steps are a good start toward implementing best practices that will greatly minimize the risks posed by consumerization within the workplace.

Step 1: Identify the Risks and Develop Policies Based on Risk Tolerance

As with any meaningful security exercise, it is important to run a risk assessment to figure out which assets your organization is trying to protect and how certain activities will put those assets at risk. Which groups of machines are more sensitive than others? Which applications are more critical to the business? How much risk can the business tolerate while accommodating line-of-business priorities regarding application and device use? These are all important questions to ask and will eventually lead your organization to better policy decisions.

This is where the balancing act begins. Perhaps your organization is willing to allow USB devices in the environment, but only those specifically chosen by the IT department and only to access certain network resources. Or maybe the organization is willing to allow the use of social media in the workplace, but only on machines that are completely up-to-date with patches and vulnerability scans.

When developing policies, organizations need to consider several key factors to best balance productivity with security and create policies that make sense for the business:

- » Corporate culture
- » IT risk tolerance
- » Productivity habits of the young workforce
- » Risks identified within your IT environment

Organizations will need to implement technology that can scan the network and examine endpoints through lightweight agents, as well as survey the user base to identify the risks currently assaulting their IT infrastructure. Once identified, decision makers can factor in culture, risk tolerance and productivity concerns to create policies that offer the best balance.

Step 2: Ensure Your Endpoints are Properly Managed

The most critical vulnerabilities introduced by the use of social media and external devices come in to play when endpoints have not been properly patched or configured. Configuration management, patch management and vulnerability management best practices will drastically reduce the rate of infection from malicious sites and content, and will diminish the amount of damage done when malware does sneak by occasionally.

Discover Assets

The first step is to survey your endpoints to find out which applications and which versions of those applications are running on your machines. Knowing what's running in your environment is critical if you ever want to completely head off risks posed by client-side applications. You can't remediate vulnerabilities within applications you don't know about.

Assess vulnerabilities and misconfigurations, and prioritize risks

As far as assessment goes, a patch management and vulnerability assessment tool should be able to help you scan those endpoints found in discovery against vulnerability sets such as BSD, CERT, CIAC, CVE, NIST, NT4_0, Network Device, Password, Password Checker, Platform Independent, Policy and QuickScan. Scans should also look for credentials that may be required to access the machines being interrogated, as well as vulnerabilities in ports, services, shares, users and groups.

Mitigate non-patchable risks

Many of the vulnerabilities that hackers target within third-party applications are part of larger blended attacks that build on additional configuration and system vulnerabilities found within the endpoint that falls victim to the attack. By addressing those vulnerabilities — many of which may not have a patch — organizations can greatly diminish the risk of an attack doing great harm, even if the attack is successful.

Organizations should seek out solutions that help them address non-patchable risks such as:

- » Open ports that can be vulnerable to attack and should be closed
- » Inappropriate firewall settings
- » Autorun CDs that can load malicious code when a CD is inserted
- » New flaws for which no patches are yet available
- » Computers with non-compliant FDCC configurations (e.g., active guest or admin accounts)

Remediating vulnerabilities

Once those policies are set, they'll need to be enforced. This is where a comprehensive third-party patch management solution is crucial. Not only can it deploy regular patches from vendors such as Adobe, Oracle and IBM, but it also provides the means to set up custom patch deployment for applications from smaller vendors.

To offer your organization the most flexibility in how patches are deployed, it is important to look for a patch management solution with some important features:

- » A reboot schedule that allows you to set reboots according to an individual agent's policies, at a specific time, or not at all
- » A sequential deployment option to minimize network traffic by breaking up patch files as they are transmitted to agents
- » A parallel deployment to distribute critical patches to multiple agents all at once
- » Quiet mode functionality that won't alert a

machine's user that a patch is being installed and does not require user interaction

- » QChain functionality to install multiple patches with one final restart (instead of rebooting after each patch)

Reporting and monitoring

Reporting on patch management and vulnerability management activities is very important for compliance activities, but perhaps even more important is its function in serving as the foundation for ongoing monitoring and discovery of new devices. Because the enterprise environment and the threat landscape are continuously changing, organizations need to think of this five-step process as a constantly rotating cycle. Robust reporting serves to feed back into future endpoint management activities.

Step 3: Establish a Trust-Centric Security Model

While patch management, vulnerability management and configuration management are important fundamentals to begin managing endpoints, organizations must also layer in alternative levels of defense to control the types of applications and devices running on the endpoints.

Application whitelisting and device controls give organizations the opportunities to keep in check the types of devices and applications running on their endpoints without completely banning new devices or locking down the deployments of applications altogether. The granularity of both tools offers organizations the ability to better balance productivity and risk by still allowing the use of known good devices (such as approved, encrypted USB drives) and applications.

Step 4: Monitor Employee Activity and Measure the Effectiveness of Your Policies

The rubber meets the road in step four. While policies are critical to mitigate the risks of consumerization, they are meaningless without some automated way to enforce them. Granularity and flexibility in policy enforcement are also important in establishing the proper balance of security vs. productivity. Organizations need to deploy the proper tools that will allow them to specifically enforce policies regarding device and application use, endpoint state and the access of data.

In addition to enforcing current policies, these tools and a little common sense need to be leveraged to make sure the organization's policies remain relevant. Policies should constantly evolve to adjust to new threats and new technology introduced to the environment.

Organizations should work to survey users about ease-of-use issues to ensure productivity isn't inhibited by current enforcement efforts, and they need to look at monitoring results and security incident metrics to measure the effectiveness of existing policy and enforcement activity in order to implement important tweaks.

Step 5: Educate the Users

Typical users are so wrapped up in their day-to-day responsibilities that they rarely think about the security ramifications of how they're using a particular piece of technology. A recent Ponemon Research study showed that one-fifth of IT decision-makers believe that employees rarely or never consider security issues when using social networking and Web applications during their workday.

The truth is that something as simple as the use of an unmanaged USB stick or the installation of an infected Facebook widget could put an entire organization's data stores at risk.

Sure, there are still those employees out there who will thumb their noses at "inconvenient" security policies and must be kept in check through automated enforcement. But many more would be amenable to adjusting their habits for the good of their employer if they just knew the whys and hows of necessary security precautions.

It is up to the IT department to educate users, both through wide-scale awareness programs and targeted education as a result of keen behavior monitoring and response to risky user activities. Proactive communication can help prevent problems caused by simple ignorance from the users.

Some examples of how the most advanced organizations are tackling user education:

- » Integrating security training with employee onboarding process
- » Establishing brown-bag lunch talks on security hot topics
- » Requiring yearly refresher security training coinciding with hire date anniversaries to update users on new policies and important security fundamentals
- » Following up with offending employees when monitoring software alerts IT about risky behavior



Example of internal training created by a customer to communicate a new policy.

Putting the Steps Together

Establishing equilibrium between worker productivity and security is no small task, and the balance will never be struck on accident. Organizations that want to arrive at that perfect middle ground between Machiavellian technology bans and ineffectual policies sans enforcement must be prepared to execute all of the steps laid out above, each of which addresses challenges particular to the consumerization of today's workplace.

Fundamental to all the steps is the classic security principle that it takes people, process and technology to keep infrastructure and data safe. Organizations need to be able to not only develop policies around Web 2.0 and removable devices; they also have to implement the necessary technology to support them and train all employees about why the rules are so important.

About Lumension Security, Inc.

Lumension Security, Inc., a global leader in operational endpoint management and 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 Compliance and Risk Management 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, Utah, Florida, Texas, Luxembourg, the United Kingdom, Germany, Ireland, Spain, France, Australia, and Singapore. Lumension: IT Secured. Success Optimized.™ More information can be found at www.lumension.com.

Lumension, Lumension Patch and Remediation, Lumension Vulnerability Management Solution, “IT Secured. Success Optimized.”, and the Lumension logo are trademarks or registered trademarks of Lumension Security, Inc. All other trademarks are the property of their respective owners.



Global Headquarters

8660 East Hartford Drive, Suite 300
Scottsdale, AZ 85255 USA
phone: +1.888.725.7828
fax: +1.480.970.6323

www.lumension.com

Vulnerability Management | Endpoint Protection | Data Protection | Compliance and IT Risk Management