

Canada

Quick Links

Home

Worldwide

Microsoft

Search Microsoft.com for:

Go

Midsize Business Center

Midsize Business Home

Information For

IT Managers

Business Leaders

Business Goals

Develop Relationships

Drive Innovation

Improve Operations

Build Connections

Industries

Products

Licensing

Security

Support

How to Buy

Software Management

Contact Us

Newsletter

Events & Webcasts

Member Services

Worldwide



How to Justify a Desktop Upgrade

Published: August 13, 2007

Summary: This article outlines how IT managers can make a case for upgrading the OS, with a focus on practical tips

Standardizing on the latest operating system and having enough RAM to support everyone's applications would make your life so much easier and more productive. It could also make your systems efficient and secure. Sounds like an easy decision, right?

But, in fact, convincing business managers to upgrade company desktops or migrate them to a newer operating system can sometimes be a very hard sell. Often, management cannot see the value in spending money on something that, from their perspective, already runs smoothly the way it is. Bruce Johnson, principal consultant with Toronto-based ObjectSharp Consulting, and a 25-year veteran of the computer industry, has spent the past 14 years on projects at the leading edge of Windows-based technology. He has some useful insights on how IT can talk to management in a language they will understand – especially when it comes to spending money in order to save money.

In Summary:

- New security features alone (such as [enhanced Group Policy capabilities](#)) can make upgrades worthwhile – know in advance what reacting to security issues is currently costing you
- When selling an upgrade, be sure to divide your reasons into clearly defined benefit “categories” (Learn how to [build an effective business case](#))
- Start slow – a phased in approach may be easier to sell than a large-scale upgrade (View other ways to help [make your software rollout successful](#))

On This Page

↓ [Security is the message](#)

↓ [The challenges](#)

Contact Us

[Contact a Microsoft Representative](#)

Member Services

■ [Not yet a Member?](#)
Find out how to access Member Services.

Resources

- [Find a Partner/Solution](#)
- [Register for Momentum, the midsize business center newsletter](#)
- [Sign up for Events & Webcasts](#)
- [Download evaluation software](#)
- [View your Microsoft License Statement](#)

↓ [The hidden cost of vulnerability](#)

↓ [Make a list](#)

↓ [Save me the money](#)

↓ [Proactive versus reactive](#)

Security is the message

According to Johnson, management may not be aware that the most compelling reason to migrate to a newer operating system, such as Windows Vista, is to take advantage of the latest security features.

"The problems with positioning upgrades is that, from a user perspective, the changes may not seem significant. But from an administrative perspective, some of the security features are huge," he said.

"So, as an IT person, who is responsible for the security of the company from viruses and for making sure that everyone is safe, there are many features in Windows Vista that I like. It does a great job of keeping people from being able to browse certain sites. It protects from viruses, because there are a lot more things that will get locked down, and the lock down tends to be tighter. You have a tougher time having things happen accidentally. Probably the biggest hassle from a security perspective [with past technologies] is that users tended to run as administrators. In Vista, that's not the default anymore."

↑ [Top of page](#)

The challenges

Johnson said upgrades can be challenging for IT as well. It requires the team to be a lot more involved in the installation and testing of the individual machines, because users are typically not going to be the administrators. Users may also be resistant to this idea at first, because they can no longer download all those fun, quirky applications that may, inadvertently, make their machines vulnerable.

"We have a bit of a Catch 22 here because, as much as people complain about their perceived lack of security, as soon as you try to do something to make it more secure, the users don't want this, because it keeps them from doing all the things that they have always done," adds Johnson.

Another challenge is the fact that the OS install requires more RAM, so IT also has to convince management to upgrade the desktops to support this. "That can be problematic for large companies, because it can get expensive."

↑ [Top of page](#)

The hidden cost of vulnerability

What management may not realize, however, is that they are already paying a hefty hidden cost by having outdated systems in place, "because you are paying for an administrator's time to deal with these issues," Johnson said. The trick is to show management this in a way that translates into dollars saved.

"It's a hard sell, because security is not a line item on their income or expense sheets. There also is not a line item that says they lost, say, \$100,000 on their security problem last year. Or lost staff productivity because people had viruses on their machines," he said.

↑ [Top of page](#)

Make a list

Johnson says as a first step, before even talking to management, IT first needs to classify and itemize the work that they do in several categories: improved productivity, security breaches, recovering from problems, etc. and then start dropping them into categories. "Once they do this, they can then start to map how much of it falls into the areas that Windows Vista, for example, may very well have been able to prevent from happening."

[↑ Top of page](#)

Save me the money

So how do you convince management to buy new machines, or upgrade the RAM and get the latest OS, if what they are doing right now seems to work OK?

Johnson said that they have to realize that they are going to have to move there eventually, in order to match the capabilities of their competitors. And once they see the cost savings they could be gaining by the increased security and productivity, they will be more open to the idea of upgrading. Even if they are not ready to do an end-to-end migration just yet, they can build the OS migration into a succession plan, and do a few machines at a time.

[↑ Top of page](#)

Proactive versus reactive

The best thing about the upgrades, once they are done, is that administrators will have more time to devote to preventing problems before they happen, Johnson said.

"The increase in security – the inability for users to just simply install stuff, means that you are decreasing the amount of reactive tasks that an administrator has to perform," said Johnson. "This allows him to become proactive in all things you want in your company."

[↑ Top of page](#)

Was this information useful?

[Manage Your Profile](#) | [Contact Us](#)

©2007 Microsoft Corporation. All rights reserved. [Terms of Use](#) | [Trademarks](#) | [Privacy Statement](#)