Your PC or the Companyâ€™s?

Posted by meggebrecht - 2009/12/16 13:41

It used to be simple: A company supplied its employees with PCs and managed them. But, as indicated by a new survey by IT services provider Unisys, those days may be becoming a thing of the past.

Of the 532 information workers Unisys surveyed, 36 percent said they prefer to bring their own PCs to work, and 19 percent prefer a hosted virtual desktop. Forty-five percent favored the traditional model. â€œTodayâ€™s multi-generational, technology-smart workforce is no longer satisfied with a restrictive model of enterprise IT support,â€• said Tony Doye, president of global outsourcing and infrastructure services at Unisys.

Employees want continual access on their own terms, according to Unisys, which cited a Gartner survey that found 43 percent of companies letting employees use their own devices at work.

Whatâ€™s your companyâ€™s policy? Are your employees and peers increasingly demanding to move beyond the traditional model? Are the challenges worth the reward?

==========

Re:Your PC or the Companyâ€™s?

Posted by epearlman - 2009/12/17 16:04

Interesting data. Now that the price of laptops has come way down, some knowledge workers may prefer to control their own destiny with their own PC. I wonder whether they expect the corporate tech support to help them if they have problems.

==========

Re:Your PC or the Companyâ€™s?

Posted by Mel Duvall - 2009/12/17 18:10

If you are allowed to use a personal laptop or similar device at work, does the company then have the right to inspect that device and its contents? It's more or less accepted that when working on a corporate PC, the company may have monitoring software in place to ensure company policies aren't being violated. I'd be curious to hear what the policy is on this front at different companies.

==========

Re:Your PC or the Companyâ€™s?

Posted by ciony - 2009/12/17 21:26

It would be interesting to know if the study had information about the size of the organization the respondents were from. My experience indicates that the practice of allowing employees to use their personal laptops, etc. tends to be more prevalent in younger/smaller organizations that don't have as many formal controls. In advocating such a policy, the IT staff at these organizations are indeed forced to contend with supporting the plethora of different devices, O/Ses, etc. since the role of IT is to maintain the productivity of the workforce, even if this practice undermines the productivity of the IT staff at a certain scale. If a company is going to go down this road, they should at least set certain minimum hardware and software requirements, especially in the anti-virus arena.

The move toward cloud computing may make the hardware used less of an issue, and as hybrid online/offline experiences like iTunes become a bigger part of people's lives it will be natural for them to want to use the same machine for personal and professional purposes. However, I think that if employees were subjected to a policy whereby the company had the right to inspect their personal PCs or require that data encryption software be installed on it, their preferences would rapidly change to having a company-provided device.

==========

Re:Your PC or the Companyâ€™s?

Posted by meggebrecht - 2009/12/17 23:37

Unisys didn't provide details on the sizes of the companies at which the surveyed employees work, though I agree that

information would be helpful in interpreting the data.

Interestingly, the Gartner survey that Unisys cites
found that 10 percent of staffers are using their own notebooks as their primary work PC, a percentage that the participating companies expect to rise to 14 percent by the middle of next year. That's fairly rapid growth, and it will make the security questions all the more pressing.

==========

Re:Your PC or the Companyâ€™s?

Posted by srw134 - 2009/12/25 17:16

I must say if I was putting my IT management hat on I would never allow workers to use their own systems at work AND use the companies network. If they wanted to use a AT&T, Verizon or Clear solution for their broadband then I would have less of a problem with it. To allow these employees to bring this amount of risk into the companies network is just a bomb waiting to go off.

-sean

==========

Re:Your PC or the Companyâ€™s?

Posted by ckaiser - 2010/01/18 10:58

Determination of technology utilization should not be an employee decision. It must be management driven, with all the relevant factors considered. Especially in regulated industries (Healthcare, financial, etc) the use of outside devices can be a major compliance violation. In other scenarios, utilization of personal hardware can be a benefit.

No one can argue that bringing outside devices such as laptops into an enterprise is a huge security risk. Unless specific security parameters are inspected and validated each time the hardware leaves and returns, you may as well just remove your firewalls and put all your company data on the internet. Once a laptop leaves the protected company network, it is subject to compromise. How do you ensure that bringing it back in won't compromise everything else?

While there are methods like central antivirus, network access protection, and personal firewalls that minimize the risks, implementing these technologies is not trivial and when you expand beyond a known dataset of hardware/software, managing the risks becomes high maintenance. It's easy for MS or Cisco to say "just implement network access protection" but the costs can be staggering.

For a business like a bank or health clinic, the answer is probably "just say no" and termination penalties for offenders. For others, there may not be any sensitive data to protect. It truly comes down to good management involvement with data security and risk management.

Employees, while often vocal about the desire to use their own devices for business, really have no say in the matter. Unless it's their business, they should be expecting to use company resources to do their work. And the companies need to provide adequate hardware to do the work, too. It does not have to be as good as the employee's new home system, as long as it provides what MANAGEMENT considers appropriate productivity. If an employee can justify to management the ROI for getting them a new beefier laptop, then perhaps they should be provided with one. But the ability to watch YouTube videos or play Halo faster isn't a business justification.

In the vast majority of cases, utilizing non-corporate assets for corporate work is a non-starter, at least where computers are concerned. There's just too much risk and the responsibility rests with upper management.

Now, cell phones are another story... ;-)

==========

Re:Your PC or the Companyâ€™s?

Posted by JohnSane - 2010/01/18 12:18

I find this to be a very interesting topic, since it lends itself to a debate about just where your personal freedoms end and a company's right to security begin. Most smaller companies, who are perceived as more nimble, sometimes look past

the limitation of security concerns to focus on the benefits of having other devices (non corporate sanctioned devices) hooking into their networks. I can see the arguement from a Corp. IT world, and from a business standpoint I think some flexibility is called for these days. Especially in a world of 24/7 business realities.

I understand more and more mobile devices will be accessing public and private clouds in the next couple of years. Most of these devices have security holes you could drive a truck through. How do you maintain security of your infrastructure and yet allow for flexibility for your work force. It is accepted that companies have a right to company email accounts, it should be accepted that companies should have a right to any personal device that would have access to the corporate infrastructure.

==========

Re:Your PC or the Companyâ€™s?

Posted by srw134 - 2010/01/29 18:33

Flexibility is well and good but when it could cost the company a great amount of money the justification just isn't there. I would however say that a good approach would be to setup a secondary network for non-corporate devices inside a company to allow some amount of device use, but this network would be outside the security of the companies network.

-sean

==========

Re:Your PC or the Companyâ€™s?

Posted by sediga - 2010/04/23 14:25

What you are saying basically calls for the company to provide an insecure network for personal access. I am not really in favor of that. I am in favor of Wireless WAN access for non-Corp validated devices. As WWAN becomes more prevalent and more widely available, the prices would drop. It would the same end result â€“ insecure accessible network â€“ but it is not provided by the company but a third party provider.

==========

Re:Your PC or the Companyâ€™s?

Posted by srw134 - 2010/04/27 03:06

Well true, I am not saying that setting up a secondary network would be my first choice but simply a choice. As I have said in other posts Wi-Max or Mobile network alternatives tend to be the best solution in these situations.

-sean

==========

Re:Your PC or the Companyâ€™s?

Posted by sediga - 2010/04/29 10:35

They are cheap too - but I would like them to be cheaper.
if a company locks down their network and not allow unauthorized copying of data, then having a WWAN connection to access personal information would not be a danger to the company. Personal freedom and security!

==========

Re:Your PC or the Companyâ€™s?

Posted by caragarretson - 2010/04/30 12:54

How do you enforce a rule of no unauthorized copying of data? How do you know when it's happened? Some organizations go as far as prohibiting thumb drives, but that sounds like throwing the baby out with the bath water. Maybe data-leak protection software?

==========

Re:Your PC or the Companyâ€™s?

Posted by rgarretson - 2010/04/30 13:24

Cell phones ARE another matter. Don't know if you noticed this, but the National Association of State CIOs recently recommended that states consider allowing employees to use personal smartphones for work. See this blog entry on it's recent report, "Security at the Edge--Protecting Mobile Computing Devices Part II: Policies on the Use of Smartphones in State Government."

==========

Re:Your PC or the Companyâ€™s?

Posted by srw134 - 2010/05/05 22:23

When it comes down to controlling the flow of data it is all about monitoring. On a typical company network people have access to the Internet and with this access can transfer files outside the companies control. If the company is dealing with data which requires a higher level of security than only internal access is allowed (and typically this is even restricted inside a specific department). The policy to disallow thumbdrives/CD's/floppies (for us old people) is nothing new it simply makes the removal of data from these higher security locations harder but not impossible.

-sean

==========

Re:Your PC or the Companyâ€™s?

Posted by sediga - 2010/05/11 13:19

It is possible to lock data down pretty tight. You would get some unhappy employees, especially developers as we need more access, but it is possible. Is it 100% bullet proof? No, but it is pretty damn close. For smaller companies, trust is key. For larger companies, it is a must.

==========

Re:Your PC or the Companyâ€™s?

Posted by mhenricks - 2010/05/11 17:18

The question of whose PC it is becomes cloudier when the employee has paid for and owns the PC and software, but the employer has essentially reimbursed the employee for the expense, and requires specific system configurations as well as adherence to security and data policies. I'm talking about "Bring Your Own Computer" which Kraft Foods recently introduced. Kraft is, by any measure, a large and sophisticated organization. Why is it okay with them when so many view it with such alarm? Could it be simple budget pressures and the desire to save 20 percent or more on purchasing and support?

==========

Re:Your PC or the Companyâ€™s?

Posted by srw134 - 2010/05/12 02:45

I had not heard about this, it is an interesting concept. However, when it comes down to it the security responsibility is on Kraft and thus they must be able to police the data and equipment connecting and transmitting on their networks. I would say that a policy would have to be put in place up front with the understanding that they (the company) control this policy and it will be created and modified based on the needs of the company.

-sean

==========

Re:Your PC or the Companyâ€™s?

Posted by caragarretson - 2010/05/12 06:03

I've heard of this Bring Your Own Computer model but I have to say I'm surprised such a big company as Kraft is supporting it. I can see the advantages -- especially if the workforce is vocal about its technology preferences and wants what they want. But so many security risks, and how to you draw the line between owned by the company and owned by the user?

==========

Re:Your PC or the Companyâ€™s?

Posted by sediga - 2010/05/12 15:02

BYOC is common for smaller companies with an IT staff of a couple of part timers. Some take the PC that I like, and turn it into a acceptable PC by installing various security software apps on it, and some just leave you alone. I believe in smaller companies, trust plays a huge factor which I can understand. I personally like that model though, mainly because I am used to a specific vendor (IBM/Lenovo), and like to stick to that. Just a preference thoughâ€¦

==========

Re:Your PC or the Companyâ€™s?

Posted by rgarretson - 2010/05/12 17:13

This seems potentially to dovetail with the cloud computing phenomenon, in which it becomes increasingly incumbent on companies and cloud vendors to find ways to lock down data within the cloud. That would seem the most efficient way to implement air-tight security, after which it doesn't matter so much -- from a security perspective, if not for end-user support -- what type or whose hardware is being used to access the data and applications. Just a thought.

--Rob

==========

Re:Your PC or the Companyâ€™s?

Posted by ckaiser - 2010/05/12 17:35

Even if data is stored within the cloud, a compromised PC can allow significant data leakage. Regardless of storage method/location, it is critical that both the company and the computer user take appropriate steps to secure data, its transfer, and the hardware accessing it.
The methodology for securing the data must be appropriate to the risk involved. For example; a credit company storing customer information including tax returns, SSNs, etc, must use a significantly more secure method of data security than a bicycle shop that only stores a product catalog and inventory details...

If I'm a bad guy and I can put a trojan on your PC without your knowledge, then any data you access anywhere is mine. That's a solid reason for any PC that has data access to be either a company owned machine or one that is "certified" by the company as being properly secured.

While DRM is a first step to protecting data, it's not foolproof. I can get around today's DRM on pretty much any PC out there. Screen capture programs, digital cameras, and other methods allow removable access to what is purported to be "secured" data.

Cloud storage is NOT a panacea for data security. In fact, it brings with it its own set of challenges. For a regulated industry, if you're going to store in the cloud, how do you PROVE to a regulator that no one at the cloud ever had access to that customer record? You can't. You have no way of knowing if someone took an image of your datafile and copied it offsite somewhere. While there are some safequards in place, the company cannot certify to regulators that their data is not accessible if it's stored in the cloud.

==========

Re:Your PC or the Companyâ€™s?

Posted by mhenricks - 2010/05/12 18:36

The Kraft policy requires employees to turn on disk encryption, which should add some security to data transported off site. I'm less clear on how the company prevents BYOCs from infecting corporate networks with viruses, malware, etc. A 20 percent savings sounds like bad deal if you have bugs running all over the place.

==========

Re:Your PC or the Companyâ€™s?

Posted by caragarretson - 2010/05/14 13:37

I wonder if Citrix's announcement of a bare metal hypervisor that runs on the client would help this issue. According to the company, the software lets users run more than one desktop virtual machine, so they can have a personal one and a corporate one. Is this the best of both worlds?

http://www.ciozone.com/index.php/Virtualization/Citrix-Shows-Off-XenClient-Virtualization-Software.html

==========

Re:Your PC or the Companyâ€™s?

Posted by mhenricks - 2010/05/14 14:09

Citrix has a vigorous BYOC program of its own, which it adopted in part because it felt it should itself be using something it was promoting to customers. Others of its products, such as Citrix Receiver, have been put for as likely to enable BYOC.

==========

Re:Your PC or the Companyâ€™s?

Posted by srw134 - 2010/05/14 23:45

It is an interesting idea but the security problems remain. I will be interested to see what the policy documents are concerning these computers being attached to company networks. What are the minimum requirements and how are they monitored. There are technologies available which can audit the PC's as they attach to ensure proper security measures before it is allowed to communicate with other computers. I would assuming these technologies would be best deployed in these instances.

-sean

==========

Re:Your PC or the Companyâ€™s?

Posted by sediga - 2010/05/16 13:50

Another possibility is the use of a VM that is â€œsavedâ€• on corporate network, and loaded on your PC when you are at work. VMâ€™s have security restrictions that wonâ€™t allow them to copy files, etc â€“ and you can use your own PC all you want. T VM is connected to corp network, and the host OS is connected via some WWAN connectivity to public network. I have setup this type of environment before, and it works very well ---

==========

Re:Your PC or the Companyâ€™s?

Posted by caragarretson - 2010/05/18 06:21

These VM and bare-metal hypervisor solutions seem like much more manageable alternatives to BYOC models. I think IT needs to ultimately have control over the systems that employees are using. Consider end of life - how does IT ensure that an old PC owned by a user but that has corporate data on it is wiped of that data and disposed of properly, if they don't own and track the asset?

==========

Re:Your PC or the Companyâ€™s?

Posted by srw134 - 2010/05/21 18:43

The bottom line for me is that I would probably not support this concept in a workplace environment, there are just to many questions. However, these types of solutions must be researched as telecommuting is becoming more and more popular.

-sean

==========

Re:Your PC or the Companyâ€™s?

Posted by sediga - 2010/05/24 11:07

Computing and computers are becoming so ubiquitous that the line between personal and work PC is all but faded away. We do need to have control over the assets, but the assets are electronic documents. If we control the access and flow of t he documents, why do you care if the PC is yours or your companyâ€™s?

==========

Re:Your PC or the Companyâ€™s?

Posted by caragarretson - 2010/05/28 09:49

That's true. I'm guessing most IT departments are used to having complete control over assets and therefore have a hard time with the idea of not owning hardware. Certainly a lot of work would have to go into establishing policies and setting standards for what the corporate desktop image is, but that's probably true in any case.

==========

Re:Your PC or the Companyâ€™s?

Posted by srw134 - 2010/05/30 00:56

I tend to agree, the thing that is lacking is a good (debatable) asset management system which secures these companies assets while they go from computer to computer as well as maintaining a record of who has them and what changes were made. Just recently, one of the companies I do work for is implementing a document tracking systems for their books which allows them to maintain a chain of control over the IP that they own.

-sean

==========

Re:Your PC or the Companyâ€™s?

Posted by sediga - 2010/05/30 08:53

In that case, it is clear what matters to a company: their IP. Personal workstations become a commodity that act as a conduit for the organization and its employees. You can use your own machine, work on companies documents and when you are done, take it home with you. The documents are saved and did not leave the premisses. I like the auditing idea as well. I have seen that done before; it is a pain to set it up, but really useful in the long run.a

==========

Re:Your PC or the Companyâ€™s?

Posted by srw134 - 2010/05/30 17:13

Well one of the things that could be extended with a good IP system is that the employees are not required to be

physically anywhere. They can work on the materials (which are checked out) at home or whereever and submit them back when they are due. An employees worth would then be rated by their ability to maintain deadlines. Of course many companies don't have the management support for this yet but as the older managers retire I believe it will get much more popular in a short amount of time. Just think of all the expenses saved by not having to house employee's. The budgets could then be focused on systems/network infrastructure, and with the remote datacenter (Cloud) technologies advancing they may evolve together quite well.

-sean

==========

Re:Your PC or the Companyâ€™s?

Posted by caragarretson - 2010/06/17 06:32

I've heard that Booz Allen is instituting a new policy this summer where employees work in the office closest to where they live, based on their zip code, regardless of which division they work for. Which I think will go a long way in employee satisfaction by cutting down on commuting and related frustrations. I've also heard that in the DC area they are piloting the idea of hoteling,which means employees work at home most of the time, and when they need an office they book one online at the local BA facility and when they show up they have everything they need. There will be upfront costs to build out the facilities to become 'hotels,' but in the long run I'm guessing the savings will be significant.

==========

Re:Your PC or the Companyâ€™s?

Posted by srw134 - 2010/06/18 20:15

Something like this is a perfect example of what I think will be the workplace of the future. There will always be some work which requires a formal office but many peoples work simply does not require this most of the time. The real question is how long will it take for people to learn the discipline required for at home work.

-sean

==========

Re:Your PC or the Companyâ€™s?

Posted by sediga - 2010/06/29 12:32

If you constitute this type of work environment, why donâ€™t you just support an all out remote workforce? It is cheaper, and with the right equipment, even more productive.

==========

Re:Your PC or the Companyâ€™s?

Posted by srw134 - 2010/07/05 14:33

I tend to agree, but with many businesses a shared home office has its purposes. I tend to thing that if it is needed and worth the cost then why not. As an independent worker I have no need for this but when I was working as a consultant for a large company a central shared office was nice (of course I was only there 10 times a year).

-sean

==========

Re:Your PC or the Companyâ€™s?

Posted by caragarretson - 2010/07/06 09:14

I agree that an all-out remote workforce would probably save money in the long run and heighten productivity (once workers got used to working at home/remote and performance goals were set accordingly) and employee satisfaction. But I think there will always be a need for some sort of office for employees to touch base, and of course to put a public

face on the company. But in general, the more the companies can keep their workforce at home - with the proper IT equipment and security precautions -- the better.

==========

Re:Your PC or the Companyâ€™s?

Posted by srw134 - 2010/07/17 15:47

This should be an interesting progression to watch. With the face of many companies shifting to their online presence the public 'brick-and-mortar' face is becoming less and less important. I look forward to this change continuing and hope that people are able to learn the proper discipline.

-sean

==========

Re:Your PC or the Companyâ€™s?

Posted by caragarretson - 2010/07/20 11:25

Yes, I think the traditional HQ office with reception area and greeter is going away...much like you often can't get a receptionist on the phone when you call main numbers these days.

==========

Re:Your PC or the Companyâ€™s?

Posted by sediga - 2010/07/20 16:00

It is easier for IT folks and mainly developers to be remote. Any customer facing position needs a presence and an office; even if the office is one room, and a shared common area between the tenants. Other than that, a remote workforce is the way to go â€“

==========

Re:Your PC or the Companyâ€™s?

Posted by caragarretson - 2010/07/22 07:15

It may be too early in this remote working trend to tell, but it would be interesting to see the cost savings a company could expect over the long term - say 5 or 10 years - from reducing physical office space, not to mention the environmental and employee-satifaction benefits. Up-front costs could be significant, not only in equipping employees with the right technology, but also is changing the company's incentive culture to promote working-at-home discipline, but I'm guessing in the longer term the company saves money.

==========

Re:Your PC or the Companyâ€™s?

Posted by srw134 - 2010/07/22 11:47

I tend to think that the big hangup is not going to be the companies offering at home work but people having problems adjusting to at home work. As a work from home person I have heard many people wish they could do a job at home full time but it does require a large amount of discipline which is not required at a physical workplace. When you are at work, the physical existence at a workplace makes people think and do the work (well, most of the time), but when you are at home many of the fun distractions which exist in your home life are available and thus harder to ignore.

-sean

==========

Re:Your PC or the Companyâ€™s?

Posted by rgarretson - 2010/11/30 20:01

Among "Gartner's Top Predictions for IT Organizations and Users, 2011 and Beyond," released today is:

By 2014, 90 percent of organizations will support corporate applications on personal devices.

"The trend toward supporting corporate applications on employee-owned notebooks and smartphones is already under way in many organizations and will become commonplace within four years," Gartner analysts predict.

Interestingly, Gartner looks beyond the upcoming "next phase of the consumerization trend," in which it is employees rather than IT that is the main driver for adoption of mobile devices (consumer-driven smartphones or notebooks, rather than "old-style limited enterprise devices") toward an even longer-term shift in "the attention of users and IT organizations from devices, infrastructure and applications to information and interaction with peers."

I'm not sure we've fully embraced this consumerization of IT, but Gartner predicts that this change in view will "herald the start of the postconsumerization era."

I can't wait!

==========

Re:Your PC or the Companyâ€™s?

Posted by srw134 - 2010/12/03 20:26

It is my personal technical opinion that they are dreaming. With the level of information security publicity lately and the continuing threat of information theft. Believing that 90% of corporations are going to open their networks to personal devices is a stretch at best, of course this also depends on their measure of what a 'corporate application' is.

-sean

==========

Re:Your PC or the Companyâ€™s?

Posted by caragarretson - 2010/12/07 19:54

I don't know that IT departments will have a choice but to support personal devices on the network. When the CEO comes in with an iPad and wants it to access corporate email, what should the answer be?

It seems the better strategy than trying to fight it might be to join it, so to speak. There are ways of securing these devices - such as third-party apps from enterprise vendors such as Cisco - so that the potential for damage is limited.

==========

Re:Your PC or the Companyâ€™s?

Posted by srw134 - 2010/12/11 20:52

Well if the CEO comes in and says I want the network to be open to these devices then fine, they think the threat is acceptable and it is their call. To believe that these devices are not a threat is naive, now I agree that there are technologies out there which can be used to secure these devices on the network, including ones that would audit the device and ensure proper policy before allowing access. However, this is assuming that the employees would want this software to run on their hardware. Inside restrictions, I have no problems allowing them to use a corporate network I am responsible for, it is unrestricted access I have issues with. As I have said in the past the other option is to just run a secondary network for those devices which are not subject to corporate policy. This is easy as the technology already exists to isolate those clients failing policy review. Any devices which use the network and fail this review could be subject to a limited access policy.

-sean

==========

Re:Your PC or the Companyâ€™s?

Posted by Petlaw - 2012/08/05 12:48

_____

The fundamental need of the company is to develop strong online presence which can only be built by the help of excellent it support. It support can prove very beneficial for any business.

_____
it support st Albans

==========

Re:Your PC or the Companyâ€™s?

Posted by alvinperez - 2012/08/28 13:54

_____

Hello..
IT companies are growing very fast in private sector. In these companies, PC's plays an important role.. I think, there is a great need to more development..

_____
Have a look at: computer repair in london

==========