An interactive eGuide

BRING YOUR OWN DEVICE (BYOD)

As more and more enterprises begin to see significant benefits from letting employees choose the device they use to get their jobs done, the Bring Your Own Device (BYOD) trend is spreading. According to the Computerworld Consumerization of IT Study published in October of 2011, about half of the 604 respondents said their organizations allow employees to do work using their own devices either away from the office or at work. Whether these devices are smart phones, tablets, or laptops that are used in the office or while working remotely, companies that embrace this trend are finding their employees are more productive and experience greater job satisfaction. What's more, enterprises can significantly reduce costs and allow for flexible work hours by letting employees use their device of choice anytime, from anywhere.

Yet BYOD presents significant security and management challenges to IT departments who want to take advantage of the trend, but still protect corporate assets. They struggle with granting users the access they need to perform their jobs, managing a wide variety of different device types, and maintaining the security of the corporate network and applications. In this eGuide, *Computerworld* along with sister publications *CIO, CSO, Network World*, and *Infoworld* examine the BYOD trend, the challenges IT departments face, and some recommendations for overcoming them.

Custom publishing from
COMPUTERWORLD

Sponsored by Good

Contents

Are CIOs Championing Consumer Tech?

Call it the great consumer embrace—or is it?

By Tom Kaneshige, CIO

NEARLY THREE OUT OF FOUR companies are adopting consumer tech, according to a report released by Avanade, a business technology services firm. This notion flies in the face of message boards and reader comments from techies condemning the practice as folly.

"There's definitely some separation of beliefs between the leaders versus the rank and file," says Ryan McCune, senior director of innovation and incubation at Avanade.

Avanade surveyed more than 600 C-level executives, business unit leaders and IT decision makers late last year. The results, Avanade says, debunk myths about the consumerization of IT. Chief among the findings is that CIOs are not hesitant to embrace consumer tech.

Moreover, companies are dedicating IT resources to managing consumer gadgets in the workplace: 91 percent of C-level executives and 75 percent of IT decision makers report that their IT departments have the staff and resources to manage the use of consumer technologies, Avanade says.

Another myth is that the consumerization of IT is largely driven by Apple products, such as the iPhone, iPad and Mac. It's true that the trend came into vogue a few years ago with the emergence of the iPhone. Chief executives brought iPhones to work and demanded IT support them.

But Avanade's survey shows that no single Apple device is even leading the charge today. The top three employee-owned devices are Android, BlackBerry, and then Apple. However, when aggregating the full portfolio of devices, Apple leads the pack, Avanade says.

Not all of the survey's findings are a boon for the consumerization of IT, especially those concerning security.

More than half of companies surveyed report experiencing a security breach as a result of consumer gadgets. Even worse, the majority of companies are not investing in training for IT staff or employees to manage the risks. •

Can Employee-Owned Devices Save Companies Money?

The costs of a 'bring your own device' enterprise deployment can be tricky to figure

By Ellen Messmer, Network World

THE "BRING YOUR OWN DEVICE" (BYOD) phenomenon is sweeping through the enterprise, and businesses such as Chicago-based design firm Holly Hunt have embraced it with gusto, offering stipends to employees to use their own mobile devices for work.

"We said, let's make this an employee benefit. If you are in a role where we issued you a corporate BlackBerry, you can if you want turn that in and carry your own device – and you'll receive a stipend," says Neil Goodrich, director of business analytics and technology at Holly Hunt, which has upscale furniture showrooms across the country as well as manufacturing and warehouse locations.

The company does require employees choosing the BYOD option to sign an agreement "that says we are allowed to reach into the device," says Goodrich, doing this with mobile management software. Several Holly Hunt employees have given up their BlackBerries in favor of personal devices, and Goodrich says the stipend, which ranges between $60 to $75 each month for employees, has so far ended up looking like a 5% reduction in cellular costs for the company.

The firm is hardly alone in embracing BYOD; a survey of 688 information and security managers done by Ponemon Institute recently found 17% of the respondents said more than 75% of the organization's employees use their personal devices in the workplace. Another 20% said more than half did. A quarter of the respondent use some kind of mobile-device management (MDM) today.

Holly Hunt requires the MDM software it selected to be installed on the employee-owned devices, and some analysts strongly support that be done especially before hooking up BYOD smartphones and tablets to corporate email, if not sooner.

Aberdeen Group analyst Andrew Borg says basic MDM controls, include device lock and wipe and adding encryption, are also going to be a requirement for some organizations. And Borg discourages a BYOD approach that would let employees select just any smartphone or tablet.

"Never say 'all,' never say 'anything goes,'" he warns. Drawing up a list of specific models of Android and Apple smartphones and tablets allowed for BYOD will go a long way in holding down costs in time and maintenance, says Borg, since IT departments will be supporting MDM software and setting security and management policies.

In its research, Aberdeen has also found that the costs related to BYOD devices, stipends and telecom are more complex than what they may seem to be at first glance.

Aberdeen found that the cost to a company from the carrier, such as AT&T, Sprint or Verizon, averages $70 per user per month for BYOD launches, while more traditional corporate enterprise deployments average $80 per user per month in direct costs, says Aberdeen analyst Hyoun Park. “At first glance, this looks like a clear win for the BYOD approach,” says Park. “However, this ignores two key points.”

First, he says, enterprise deployments can be highly optimized through rate plans, contract negotiations, and ongoing cost management practices associated with best-in-class wireless expense management. “Aberdeen finds that these practices typically result in over 25% savings and many of these practices cannot be performed in a direct fashion through BYOD deployments,” Park claims.

“Second, there is typically a high degree of overhead associated with compensating BYOD users,” says Park, noting the majority of BYOD users are reimbursed through monthly expense reports. Aberdeen research shows that the average total cost associated with processing an expense report is $29, making the average total cost per month $99. However, because this management cost is typically hidden to the enterprise, it is typically not considered in context of the total cost of BYOD, Park points out. “In contrast, the total cost of expense management for a formally managed enterprise mobile device is typically around $5 per month,” he notes, for a total corporate average of $85 for non-BYOD.

“There’s no vendor in the telecom management expense management space that has come up with an elegant approach to aggregate BYOD billing,” Borg adds. “Bills are getting disaggregated because of BYOD,” he says. Consequently, businesses embracing BYOD may be giving up the ability to aggregate the bills.

For these reasons, though it may seem that costs have shifted to the employee, the opposite may be occurring as operational costs are actually going up because of BYOD.

BYOD is here to stay

However, it’s unlikely that BYOD is a passing phenomenon. Borg notes that while it may be seen as a disruptive change, driven by the employee enthusiasm for new technologies, it can be utilized effectively through clear planning.

But more challenges appear to arise from the “dual-use” device that BYOD engenders as one employee-owned mobile smartphone or tablet is carried for both business and personal communication. For one, how will business and personal apps be differentiated; how will sensitive business data be cordoned off from personal use?

Newer mobile virtualization approaches put forward by VMware and Citrix, though not yet widely deployed, will be among possibilities that businesses examine to create “dual-use” mobile devices. But other choices are also there to be explored. •

Market Trend

BYOD Movement is Forcing IT to Adapt

But user empowerment still allows IT to assess apps and manage mobile devices By Paul Krill, InfoWorld

IT DEPARTMENTS in the age of mobile computing must adapt to newly empowered users who select not only their own devices but their applications as well. This adaptation – as difficult as it may seem – has a strong benefit: Enabling a modern workforce, said Maribel Lopez, president of Lopez Research at the AppNation conference last week in San Francisco.

"You can look at it [from the perspective that] BYOD is taking control away from IT, or you can look at it as it's an opportunity to mobilize your entire business that you would have never been able to afford before because you wouldn't have bought the devices and you wouldn't have wanted to manage them," Lopez said. Her advice to IT: "Accept that BYOD is happening and build a plan around it – how to manage it, how to secure it, how to get apps to devices."

Users are bringing in their own devices and choosing applications such as Box.net for file sharing and DocuSign for electronic document signatures, without waiting for IT signoff, noted Ken Singer, CEO of MDM (mobile device management) provider ApCentral. "CMOs and CEOs were coming in with their own iPads and demanding that the IT departments support these devices."

Such pressures mean a new reality for IT, a reality many will not like, Singer said. He likened IT's crumbling power vis à vis mobile adoption to last year's "Arab spring," in which people in Middle Eastern countries rose up against entrenched, autocratic leaders. "IT is struggling with how to address this, how to look at this, and what they should do to respond because they can't simply say yes to everything," he said. "They can't manage it all."

IT must understand that businesspeople are going to build applications, with mobile applications serving as a catalyst for changes, said Ojas Rege, vice president of products and marketing at MDM provider MobileIron. "In the past, the business wanted apps, but they just didn't have the mechanism to build them." Instead, they had to rely on line-of-business applications, such as SAP or Siebel. "Now, it's really easy for them to go and build them or buy them," Rege said.

IT is concerned that such "foreign" apps create security risks, but Lopez said that MDM and mobile application management tools can let IT departments be more flexible about such apps. However, she argued that flexibility did not mean a free-for-all: "Some apps today are not appropriate." •

Opinion

Risky Workers

Are your policies and enforcement efforts keeping up with consumerization? By Bob Bragdon, CSO

I THOUGHT WE COULD examine a recent theme in a little more detail: the challenges of dealing with the consumerization of IT devices in the workplace. We recently completed a study, in partnership with Symantec, that looked at the security and compliance risks of a mobile workforce. It affirmed what I've believed for a long time, namely, that there is a consensus that mobile workers pose a great risk and that, for the most part, businesses are not prepared to mitigate that risk.

Today, every business has a mobile workforce of one form or another. The larger the organization, the greater the challenge. And this mobile workforce is important. Most businesses understand the benefits of untethering their employees and pushing corporate resources out into the field. But as these workers carry corporate data outside the traditional enterprise, they increase the risk of loss, theft or misuse.

Although businesses have gotten pretty good at protecting their laptops, the challenge grows exponentially as more and more devices (iPads, Android devices, and so on) are introduced into the equation. Most businesses are still coming up short in their efforts to protect these devices—not just from a technical standpoint, but also from the point of view of enforcing corporate policies that govern the acceptable use of mobile devices.

Most businesses surveyed do not use any technological solutions to enforce compliance with corporate acceptable-use policies (monitoring and enforcement, as we all know, are key tenets of a good security program—the old "trust but verify" axiom).

There are a variety of reasons that businesses haven't adopted solutions to address this issue; the most common are related to budget and resource constraints, and where this issue falls in the pecking order of security priorities. But at the same time, 91 percent of survey respondents believe that there is a significant likelihood that mobile employees will violate their acceptable-use policies.

But if you are not willing to accept violations of acceptable-use policies among tethered workers, why do you accept violations from mobile workers? With a clear understanding of the risks, security executives need to be more proactive in addressing these security shortcomings so they can protect their organizations from compliance missteps.

Failing to do so is quickly becoming a mistake that businesses cannot afford to make. •

Security Manager's Journal: BYOD Planning Gets a Big Boost

A key technology to allow for the secure use of personal devices on the network is virtual desktop infrastructure **By Mathias Thurman, Computerworld**

WE'RE MAKING BIG STRIDES toward our CIO's goal of enabling a "bring your own device" (BYOD) policy. For me, it's none too soon.

That's because employees are increasingly finding ways to connect their own Macs, tablet PCs, and other mobile devices to our internal corporate environment, both from within the office and remotely. In the absence of a policy, it's been a case of anything goes as long as you don't get caught. By embracing this trend and setting up guidelines, we stand a chance of controlling what's connected to our network and securing our environment.

One important technology that will make this work is virtual desktop infrastructure, commonly referred to as VDI – if it's deployed in a secure manner, that is. I met with the VDI project team to make sure that's how it happens.

One of the benefits of allowing only known devices to connect to your network is that you can track a PC to a user and location because you know all the IP addresses, machine names, and MAC addresses that are permitted. With VDI, we can expand the pool of devices that can connect to the network because the VDI will identify the user. If, for example, some piece of malware enters the network, we can use our audit and event logs and our security incident and event management tool to track down the source.

We plan to allow VDI access from untrusted environments – for example, a PC at an Internet kiosk halfway around the world. One of my requirements is that we enable a sandbox mode to ensure that there is no possibility of direct interaction between the untrusted PC and the VDI environment. This way, malware can't be uploaded to the trusted VDI environment, and intellectual property can't be downloaded to the PC. (Some of these restrictions can be waived if the VDI determines that the remote PC is, in fact, a company asset.) I also want aggressive settings for session timeout and screen lock, to mitigate the problems that arise when forgetful workers walk away from a kiosk without logging out of the VDI.

VDI could also be helpful in managing the access of our contingent workforce. This includes vendors, partners, suppliers, distributors, contractors, and consultants. Some of these people need access to our infrastructure and applications, but providing them with a VPN client can be a logistical nightmare, since varying levels of access are needed for each engagement. VDI will allow us to set up a “rule of least privilege” (one of my primary security philosophies) for all of our contingent workers. Once again, this will help protect our infrastructure and limit the compromise of our intellectual property.

Security Ground Rules

I also told the project team that we need a login banner notifying users that they have no expectation of privacy. Our legal department has demanded that we force users to click a box indicating that they accept the possibility that the company might monitor their activity.

Another of my requirements is that there be no residual data pertaining to VDI activity on the host PC after a user has logged out. This will be especially important when the PC is untrusted (like one used in an Internet cafe, for example). In addition, the VDI environment must be integrated into Active Directory, so we can easily make the VDI unavailable to former employees and current employees who no longer need access.

Finally, as with all remote connections, any access to the VDI environment must be encrypted and require two-factor authentication.

This journal is written by a real security manager, “Mathias Thurman,” whose name and employer have been disguised for obvious reasons.

Opinion

The Interesting Bits ... and Bytes

Consumer tech and IT: Not always a good marriage By Barbara Krasnoff

THE CONSUMERIZATION OF IT is one of the topics of great interest in enterprise these days. The ability to allow employees to use their own smartphones, tablets, etc. to work with – rather than issuing equipment that may not be as current as they would wish, forcing people to either work with older devices or carry two sets of devices with them – is a laudable one. But the problem is how to marry the two without causing the kind of clash that leads to a rather nasty divorce.

I was thinking about this when a close friend acquired a new Android Galaxy Nexus smartphone and decided that it would be a good idea to use it to pick up her work email – especially as she was about to travel to CES in Las Vegas and would be doing most of her work from her smartphone. She contacted her IT department, which sent her clear instructions on how to configure her phone. So far so good.

The first hurdle appeared when she discovered that she would have to give her IT department full administrative permission to, among other things, wipe the complete contents of her phone. She called IT.

“Don’t worry,” the IT staffer told her. “We’d only do it in extreme situations – if the phone was lost or if you left the company”

“If I left the company?” she asked. “This is my personal phone. Why do you get to wipe the whole thing if I leave the company?”

“You should be backed up,” was the simple answer.

This was bothersome enough, but when she finally decided to grit her teeth and accept the necessity of giving her company full access to her personal smartphone, another hurdle appeared – one that wasn’t as easy to get over. As the last part of the process, she was required to have the complete contents of her phone encrypted – and there was no way to simply undo the process. In order to unencrypt her data, she’d have to do a hard reset. Everything would be lost.

“And what about other apps?” she asked. “Will the encryption interfere with installing new apps?”

There was no firm answer. And that was the end of that – the divorce of my friend’s new smartphone and her business email was complete. She decided to struggle along with Webmail and her personal Gmail. Thus making her job harder – and making it less likely that her company would be able to communicate with her as efficiently as possible.

Security is necessary, especially when dealing with corporate information – but when employees are purchasing expensive smartphones partly in order to make their daily work easier and even possible, organizations have to make it possible for those employees to feel comfortable dealing with those security restrictions. Or start investing in the technology themselves. •

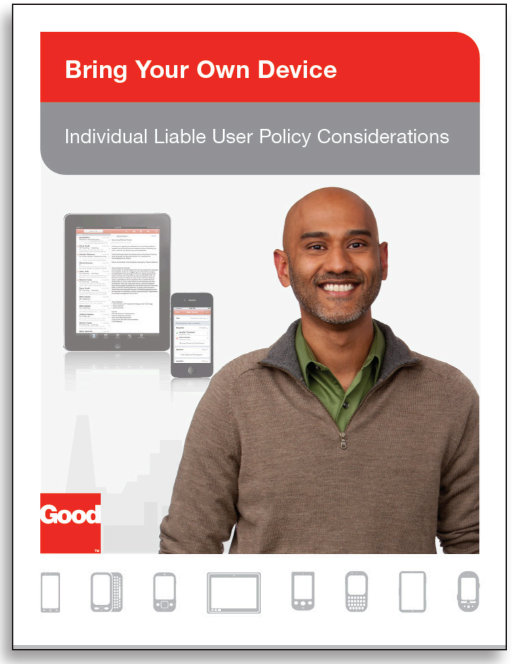
Resources

White Paper

BYOD: How to Design Secure Usage

With employee mobile devices springing up throughout your workplace, how can you establish an individual liable usage policy? Use these questions from Good Technology to help prepare your organization for eligibility, reimbursement, security, and acceptable use considerations, as well as end-user support and policy violation issues.

▶ **Download**



Bring Your Own Device

Individual Liable User Policy Considerations

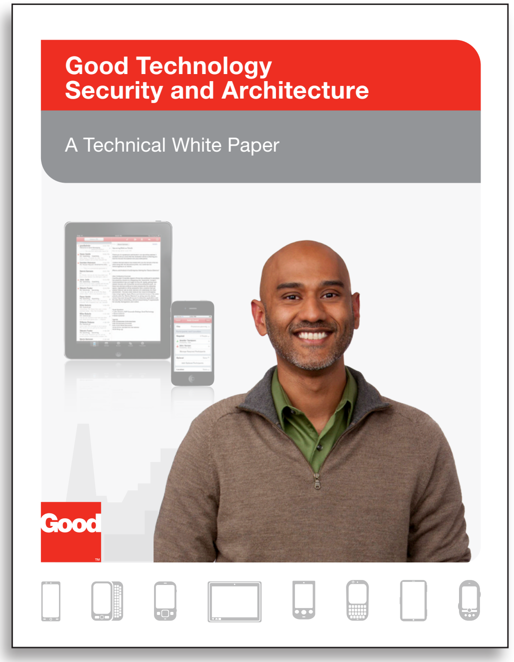
Good

White Paper

Protect Company Data & Employee Privacy

Rather than limiting device choice, smart businesses are finding ways to protect enterprise data integrity and employee privacy on popular mobile devices. Good Technology helps companies embrace business mobility by delivering a multi-layered security model that addresses the safety of data in every part of the mobile infrastructure.

▶ **Download**



Good Technology Security and Architecture

A Technical White Paper

Good