



BYOD POLICY IN THE ENTERPRISE



6 TRENDS DRIVING BYOD POLICIES AND WHY LATE ADOPTERS ARE GETTING LEFT IN THE DUST

There's a good chance the future success of your business is already in your pocket. Consumers everywhere are using smartphones and tablets to handle everything from banking on the go to connecting via IM, email and social media. As devices pour into the enterprise, businesses can leverage the Bring Your Own Device (BYOD) trend as a way to reduce costs, increase productivity and enhance communication and collaboration. The challenge is saying yes to BYOD while maintaining control of your network, information security, communications privacy and devices.

BYOD is happening whether businesses like it or not. In 2012, 53% of information workers used their own devices for work.¹ And it's not just younger workers and new hires who are bringing their own devices. In most enterprises, executives and high-level employees are doing business from their own devices as well. By the end of 2011, 77% of executives brought their own hardware to work, and 45% brought their own software.¹ According

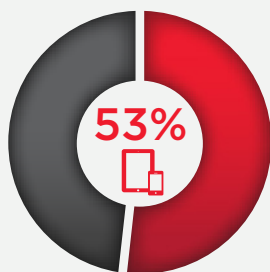
to a Gartner survey of global CIOs, 38% of companies expect to stop providing devices to employees and instead will require BYOD by 2016.²

As more employees show up with their own mobile devices, the line between personal and professional equipment is blurring. Because business networks are involved, however, a whole host of security, privacy and other issues arise when addressing BYOD. And if

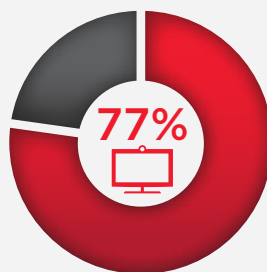
businesses don't address all these issues quickly, they are likely to fall behind more agile organizations in areas such as recruitment, retention, employee productivity, accessibility and customer satisfaction.

The question isn't whether BYOD is happening but whether you are managing it and leveraging the additional computing power to your company's advantage.

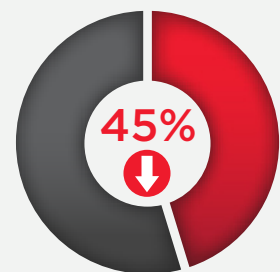
Studies show that corporate workers are bringing their own tools to the job.



53% of information workers used their own devices.¹



77% of executives brought their own hardware.¹



45% of executives brought their own software.¹

This paper outlines the six trends that are forcing businesses to address BYOD and offers tips that should be considered when setting a new BYOD policy.

1. PRODUCTIVITY WITH ENTERPRISE LEVEL COMMUNICATIONS

One of the primary drivers for employees to use their own devices at work — and one of the biggest reasons for businesses to encourage this — is increased productivity. Anywhere accessibility to enterprise-level communications and applications can lead to higher efficiency and profitability. Always-on virtual offices delivered through BYOD solutions enable rapid engagement with workers and experts, which helps address problems more quickly and improve customer satisfaction.³ A full 70% of firms in a 2012 Forrester study increased their bottom line revenues as a result of deploying BYOD programs.⁴

2. INFRASTRUCTURE


Growing demand for mobility is pushing businesses to figure out how to adapt their existing networks. Business networks can be strained by the addition of new, more collaborative mobile applications and devices. In fact, older networks might not be able to handle them at all. This is why IT professionals taking on BYOD with an outdated network can face an endless stream of technical issues that are unsustainable from a cost perspective.


Today, forward-looking IT organizations must first make sure their wired and wireless networks support greater capacity, performance and resiliency. They must also ensure that their networks are optimized to support real-time applications like voice and video. And, to support anywhere, anytime collaborative communications, they need to migrate their existing network to a Session Initiation Protocol (SIP) based communications infrastructure that will accommodate a wide range of devices and help generate the needed cost savings to self-fund the investment.

3. MOBILE WORKFORCE

50% of information workers work from multiple locations.⁵

Half of all information workers in a 2012 Forrester survey said they are now working from multiple locations.⁶ New technology such as smartphones and Internet-connected tablets enable workers to work and collaborate on the move, but they don't always allow fully connected communication. Computing power, storage, display and video capabilities, and even battery life can disrupt workflow. This is why businesses coming up with BYOD policies should consider the technical limitations of devices employees are allowed to use. They should also make sure their communications and IT systems are capable of supporting the growing number of mobile workers.

80% 
of enterprises with BYOD policies report an increase in productivity.³

60% 
of workers report higher productivity when using their own devices.⁵

“Many businesses find that by enabling workers to do more, having a BYOD solution helps them to address problems faster and improve overall customer satisfaction.”²

4. COMPATIBILITY

Employees want the power to select their own devices. Currently 45% want to choose their own smartphone and 40% want to choose their own tablet.⁷ Of course, IT departments need to make sure these preferred devices work on their business networks. They must also make sure devices work with each other. One-third of IT decision-makers said the biggest barrier to implementing mobile

solutions was finding ways to seamlessly integrate different operating systems. For some mobile collaboration applications such as video conferencing, businesses need to support compatibility across any mobile device their employees use as well as different platforms used by their customers, partners or guests when these individuals need to be part of a collaborative effort.

5. SECURITY

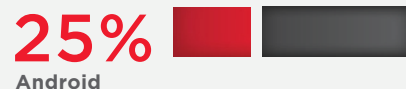
Partners or guests visiting an organization can create thousands of potential weak points in a business network. Managing who, what, where and when individuals can access the business network and its information is essential. Also, since sensitive information leaves a company's network with employees on a daily basis, it's important to put safeguards in place since any lost mobile phone or tablet could become a potential security leak. The key to keep in mind

when considering BYOD policies is that allowing personal devices doesn't mean allowing *all* personal devices. Businesses should build policies around their security needs, enforce role-based network access policies and provide a list of permitted devices that meet the security standards, including a strategy to address remediating devices that are out of compliance. Successful policies will also account for the data on devices that leave the organization's control.

6. HR AND LEGAL ISSUES

BYOD is not just an issue for the IT department. Since managing corporate data on private devices involves privacy laws, employees who bring personal devices to work become potential liabilities for the business. Personal information on employee devices needs to be kept off business networks in order to protect the privacy of employees, but likewise, certain

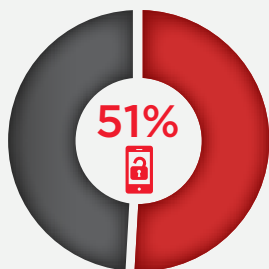
Devices Information Workers Use at Work⁶



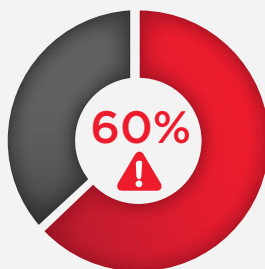
types of corporate information needs to be kept safe from employees. Of course, multinational companies need to address the privacy laws of *all* the countries in which they operate.

In recent years, hackers — who may have been thwarted by VPNs, firewalls, virus detectors and other security measures — have been turning their attention to the many smartphones and tablets in the enterprise. This can pose huge legal problems to executives. With today's industry security mandates holding them responsible for security breaches that expose customer information and corporate data, businesses can incur financial penalties as high as \$50,000 per violation with a maximum of \$1.5 million per year.¹⁰

Security becomes an important issue in a mobile workforce.



51% of IT professionals reported security breaches from unsecured mobile devices.⁸



60% of IT professionals saw increased malware infections from unsecured mobile phones.⁹

WHAT TO CONSIDER FOR NEW POLICIES

Customized Approaches

One-size-fits-all won't work with BYOD. Not all businesses have the same needs. In order to develop effective policies, businesses should identify the employee roles that can benefit from BYOD and what devices should be involved. Solutions should be developed with legal and HR in mind so that the protection of employee privacy is taken into account.

It's important to remember that developing a BYOD policy should be an evolutionary process. The BYOD trend is happening on its own, and the most effective policies will develop naturally as organizations find solutions to their own unique IT problems. When developing a customized approach, organizations should form a team with stakeholders from IT, HR, legal, accounting and security in order to identify specific needs. Once a plan is developed, IT will need to learn what works, make adjustments and adapt the plan as needed along the way.

52% of information workers use three or more devices.³

Security Plans

Security plans are essential when developing a BYOD policy. Having no BYOD solution is the biggest security risk of all for an organization because people are accessing the network without limitations in place. However,

there's much to consider when addressing the blurring of personal and professional spaces. Security architectures that involve app-by-app permission instead of device-wide permission allow devices to stay in the employee's hands while still having restrictions on sensitive information.

Another good option are virtualization solutions that allow users to access cloud-based applications or file systems using standard, broadly available web browsers. Virtualization solves the problems that come up from divergent operating systems or device types since the actual applications run on a server that is accessed through mobile applications. This simplifies matters and can be a more economical approach since it avoids the support required by client-based applications that would have to be deployed on an individual-by-individual basis.

User-Defined Plans

Not all employees have the same needs. This is why most businesses can enhance their security plan by incorporating a complementary, centrally managed, network access solution that authenticates and authorizes individual users, guests and devices over a wide range of role-based access options. This solution allows businesses to restrict access to business information, applications and network resources based on the role of the individual. It also allows the business to cut off all access after devices or employees leave the company. This keeps access to information secure and helps make sure employees are working according to the needs of the business.

The Shift to BYOIT

BYOD is only the start of blending personal and professional technology. The next step is "Bring Your Own IT." Workers will soon be bringing entire ecosystems with them to

“Workers will soon be bringing entire ecosystems with them to work — social networks, applications and collaboration tools.”

work — social networks, applications and collaboration tools. The increase in consumer computing power means employees are also beginning to bring their own PCs to work. By introducing policies that address BYOD now, businesses can put themselves in position to address more technology crossing into the workplace. Going forward, businesses will need to carefully try out new technology to see if it fits into their business and how.

Preparing for Bring Your Own Applications

With employee-owned devices come consumer apps and services. As more outside mobile devices and computers show up in the workplace, programs not meant for enterprise use will also start popping up on company networks. Employees rely on apps they're familiar with — such as Dropbox, Google Docs and Skype — to work the same way they would away from work. These apps are easy to use and readily available, but they also bring a new set of potential data security problems. IT departments should recognize the benefits of these apps — and employee preferences — and look for ways to fit them into security policies in a way that doesn't put the enterprise at risk.

Solutions from AVAYA

Avaya offers comprehensive solutions that help you manage the many challenges of BYOD. Avaya's approach spans employee needs, locations, devices and services through a variety of solutions:

- **Identity Engines** allow businesses to centrally manage and secure network access using the network to authenticate and authorize individual users, guests and devices over a wide range of role-based access options. With a BYOD initiative, business can now control network access based on who they are, what they can access, and where and when they have access.
- **Session Border Controllers** enable the safe use of personal mobile devices by securing Session Initiation Protocol (SIP) applications and enabling remote workers without cumbersome Virtual Private Networks (VPNs).
- **Remote Office Clients** solve security and mobility issues by allowing users to connect to virtual desktops and switch between devices to access information.
- **UC Solutions** create virtual offices that keep business moving. Enterprise-level business applications allow users to connect and collaborate whether they're traveling, at a customer site or working remotely.
- **Networking Solutions** help companies meet growing bandwidth needs and enable roaming employees with optimized, secure wireless networking.
- **Avaya Aura® SIP-based UC solutions** create a truly mobile workplace by enabling voice, video and text-based collaboration capabilities, regardless of location or switch connection.
- **Avaya SIP Transformation Services** help businesses develop the economic justification to modernize and migrate their current communications framework to SIP. Avaya consultants identify new business benefits and cost savings to help you self-fund your investment to switch to more collaborative communications.

“As more outside mobile devices and computers show up in the workplace, programs not meant for enterprise use will also start popping up on company networks.”

Learn more about how Avaya addresses BYOD needs. Visit avaya.com/mobility or call **1-855-206-4636**.

¹Forrester, *Forrsights Workforce Employee Survey*, Q4 2011, 2012

²Gartner, *Bring Your Own Device: The Facts and the Future*, 2013

³Forrester, *Connected Mobile Workers Power Innovation to New Heights*, 2012

⁴Forrester, *Key Strategies to Capture and Measure the Value of Consumerization of IT*, 2012

⁵Forrester, *BYOD in Government: Prepare for the Rising Tide*, 2012

⁶Forrester, *Mobile Solutions Connect Information Workers to Collaboration and Innovation Processes*, 2012

⁷Forrester, *Mobile Application Adoption Trends and Strategies to Engage the Workforce*, 2012

⁸Avaya, *As Threats Persist, IT Security Gains Higher Awareness Among C-Level Executives and Board Members*

⁹Ponemon Institute, *Global Study on Mobility Risks*, 2012

¹⁰American Medical Association, *HIPAA Violations and Enforcement*, from the American Recovery and Reinvestment Act, 2009