Bring your own device

Bring Your Own Device (**BYOD**)—also called **bring your own technology** (**BYOT**), **bring your own phone** (**BYOP**), and **bring your own Personal Computer** (**BYOPC**)—refers to the policy of permitting employees to bring personally owned devices (laptops, tablets, and smart phones) to their workplace, and to use those devices to access privileged company information and applications.[1] The phenomenon is commonly referred to as IT consumerization.[2]

BYOD is making significant inroads in the business world, with about 75% of employees in high growth markets such as Brazil and Russia and 44% in developed markets already using their own technology at work.[3] Surveys have indicated that businesses are unable to stop employees from bringing personal devices into the workplace.[4] Research is divided on benefits. One survey shows around 95% of employees stating they use at least one personal device for work.[5]

History

The term BYOD first entered common use in 2009, courtesy of Intel when it recognized an increasing tendency among its employees to bring their own devices (i.e., smartphones, tablets and laptop computers) to work and connect them to the corporate network.[6] However, it took until early 2011 before the term achieved any real prominence when IT services provider Unisys and software vendor Citrix Systems started to share their perceptions of this emergent trend. BYOD has been characterized as a feature of the "consumer enterprise" in which enterprises blend with consumers.[7] This is a role reversal in that businesses used to be the driving force behind consumer technology innovations and trends.[8]

In 2012, the U.S.A Equal Employment Opportunity Commission adopted a BYOD policy, but many employees continued to use their government-issued BlackBerrys because of concerns about billing, and the lack of alternative devices.[9]

New trends

The proliferation of devices such as tablets and smartphones, which are now used by many people in their daily lives, has led to a number of companies, such as IBM, to allow employees to bring their own devices to work, due to perceived productivity gains and cost savings.[10] The idea was initially rejected due to security concerns but more and more companies are now looking to incorporate BYOD policies, with 95% of respondents to a BYOD survey by Cisco saying they either already supported BYOD or were at least considering supporting it.[11]

This new trend also prevents IT from having to continuously keep up with new technology available on the market, which in recent years has become a complex and constantly growing challenge.

Prevalence

The Middle East has one of the highest adoption rates (about 80%) of the practice worldwide in 2012.[12]

According to research by Logicalis, high-growth markets (including Brazil, Russia, India, UAE, and Malaysia) demonstrate a much higher propensity to use their own device at work. Almost 75% of users in these countries did so, compared to 44% in the more mature developed markets.[13]

In the UK, the CIPD Employee Outlook Survey 2013 revealed substantial variations by industry in the prevalence of BYOD.

Advantages

Some reports have indicated productivity gains by employees.[14] Companies like Workspot inc believe that BYOD may help employees be more productive.[15][16] Others say it increases employee morale and convenience by using their own devices and makes the company look like a flexible and attractive employer.[17] Many feel that BYOD can even be a means to attract new hires, pointing to a survey that indicates 44% of job seekers view an organization more positively if it supports their device.[18]

Some industries are adopting BYOD quicker than others. A recent study[19] by Cisco partners of BYOD practices stated that the education industry has the highest percentage of people using BYOD for work at 95.25.

A study[20] by IBM says that 82% of employees think that smartphones play a critical role in business. The study also shows benefits of BYOD include increased productivity, employee satisfaction, and cost savings for the company. Increased productivity comes from a user being more comfortable with their personal device; being an expert user makes navigating the device easier, increasing productivity. Additionally, personal devices are often more cutting edge as company technology refreshes don't happen as often. Employee satisfaction, or job satisfaction, occurs with BYOD by allowing the user to use the device they have selected as their own rather than one selected by the IT team. It also allows them to carry one device as opposed to one for work and one for personal use. Cost savings can occur on the company end because they now would not be responsible for furnishing the employee with a device, but is not a guarantee.

Disadvantages

Although the ability to allow staff to work at any time from anywhere and on any device provides real business benefits; it also brings significant risks. To ensure information does not end up in the wrong hands, it’s imperative for companies to put security measures in place.[5] According to an IDG survey, more than half of 1,600 senior IT security and technology purchase decision-makers reported serious violations of personal mobile device use.[21]

Various risks arise from BYOD, and agencies such as the UK Fraud Advisory Panel encourage organisations to consider these and adopt a BYOD policy.[22][23]

BYOD security relates strongly to the end node problem, wherein a device is used to access both sensitive and risky networks/service risk-averse organizations issue devices specifically for Internet use (this is termed

Inverse-BYOD).[24]

BYOD has resulted in data breaches.[25] For example, if an employee uses a smartphone to access the company network and then loses that phone, untrusted parties could retrieve any unsecured data on the phone.[26] Another type of security breach occurs when an employee leaves the company, they do not have to give back the device, so company applications and other data may still be present on their device.[27]

Furthermore, people sometimes sell their devices and might forget to wipe sensitive information before selling the device or handing it down to a family member. Various members of the family often share certain devices such as tablets; a child may play games on his or her parent's tablet and accidentally share sensitive content via email or through other means such as Dropbox.[28]

IT security departments that wish to monitor usage of personal devices must ensure that they only monitor work related activities or activities that accesses company data or information.[29]

Organizations who wish to adopt a BYOD policy must also consider how they will ensure that the devices which connect to the organisation's network infrastructure to access sensitive information will be protected from malware. Traditionally if the device was owned by the organisation, the organisation would be able to dictate for what purposes the device may be used or what public sites may be accessed from the device. An organisation can typically expect users to use their own devices to connect to the Internet from private or public locations. The users could be susceptible from attacks originating from untethered browsing or could potentially access less secure or compromised sites that may contain harmful material and compromise the security of the device.[30]

Software developers and device manufacturers constantly release security patches due to daily increase in the number of threats from malware. IT departments that support organisations with a BYOD policy must be prepared to have the necessary systems and processes in place that will apply the patches to protect systems against the known vulnerabilities to the various devices that users may choose to use. Ideally such departments should have agile systems that can quickly adopt the support necessary for new devices. Supporting a broad range of devices obviously carries a large administrative overhead. Organisations without a BYOD policy have the benefit of selecting a small number of devices to support, while organisations with a BYOD policy could also limit the number of supported devices, but this could defeat the objective of allowing users the freedom to completely choose their device of preference.[31]

Several market and policies have emerged to address BYOD security concerns, including mobile device management (MDM), containerization and app virtualization.[32]

While MDM provides organizations with the ability to control applications and content on the device, research has revealed controversy related to employee privacy and usability issues that lead to resistance in some organizations.[33] Corporate liability issues have also emerged when businesses wipe devices after employees leave the organization.[34]

A key issue of BYOD which is often overlooked is BYOD's phone number problem, which raises the question of the ownership of the phone number. The issue becomes apparent when employees in sales or other customer-facing roles leave the company and take their phone number with them. Customers calling the number will then potentially be calling competitors which can lead to loss of business for BYOD enterprises.[35]

International research reveals that only 20% of employees have signed a BYOD policy.[36]

It is more difficult for the firm to manage and control the consumer technologies and make sure they serve the needs of the business.[37] Firms need an efficient inventory management system that keeps track of which devices employees are using, where the device is located, whether it is being used, and what software it is equipped with.[37]

If sensitive, classified, or criminal data lands on a U.S. government employee's device, the device is subject to confiscation.[38]

The USMC is seeking to outsource the security requirements of their BYOD policy to commercial carriers such as Sprint, Verizon, and AT&T.[39]

Another important issue with BYOD is of scalability and capability. Many organisations today lack proper network infrastructure to handle the large traffic which will be generated when employees will start using different devices at the same time. Nowadays, employees use mobile devices as their primary devices and they demand performance which they are accustomed to. Earlier smartphones did not use a lot of data and it was easy for Wireless LAN to handle that amount of data, but today smartphones can access webpages as quickly as most PCs do and have applications that use radio and voice at high bandwidths, hence increasing demand from WLAN infrastructure.

Finally, there is confusion regarding the reimbursement for the use of a personal device. A recent court ruling in California indicates the need of reimbursement if an employee is required to use their personal device for work. In other cases, companies can have trouble navigating the tax implications of reimbursement and the best practices surrounding reimbursement for personal device use.

Personally owned, company enabled (POCE)

A personally owned device is any technology device that was purchased by an individual and was not issued by the agency. A personal device includes any portable technology like camera, USB flash drives, mobile wireless devices, tablets, laptops or any personal desktop computer.

The agency will maintain management control and authorize the use of personally owned devices and shall develop guidelines to define which employees can use their own devices, the types of devices they can use, and which applications and data they can access, process, or store.[40]

Corporate owned, personally enabled (COPE)

As part of enterprise mobility, an alternative approach are corporate owned, personally enabled devices (COPE). With this policy the company purchases the devices to provide to their employees; the functionality of a private device is enabled to allow personal usage.

The company maintains all of these devices similarly to simplify its IT management; the organization will have permission to remotely delete all data on the device without incurring penalties and without violating the privacy of its employees.

Other policy considerations

BYOD policies can vary greatly from organization to organization depending on the concerns, risks, threats, and culture. As such, BYOD policies can differ in the level of flexibility given to employees to select device types. Some policies may dictate a narrow range of devices; others may allow a broader range of devices. Related to this, policies can be structured to prevent IT from having an unmanageable number of different device types to support. It's also important to clearly state what areas of service and support are the employees' responsibilities versus the company's responsibility.[41]

BYOD users often get help paying for their data plans with a stipend from their company. Also, there may be a policy aspect as to whether an employee should be paid overtime for answering phone calls or checking email after hours or on weekends. Additional policy aspects may include how to authorize use, prohibited use, perform systems management, handle policy violations, and handle liability issues.[42]

For consistency and clarity, BYOD policy should be integrated with the overall security policy and the acceptable use policy.[41] To help ensure policy compliance and understanding, a user communication and training process should be in place and ongoing.

See also

- Bring your own encryption

- Bring your own operating system
- Mobile security
- One to one computing
- Remote mobile virtualization

References

1. ^ It interrupts the class BYOD on pcworld.com
2. ^ *"Enterprise & Gateway Suites - Trend Micro". Trend Micro.*
3. ^ *"BYOD – Research findings". Logicalis. Retrieved 12 February 2013.*
4. ^ Rene Millman, ITPro. "Surge in BYOD sees 7/10 employees using their own devices." Aug 12, 2012. Retrieved Jun 5, 2013.
5. ^ ***a b*** http://www.vodacom.com/com/press/detail?articleId=4224
6. ^ *"Mobile: Learn from Intel's CISO on Securing Employee-Owned Devices". Gov Info Security. Retrieved 10 January 2013.*
7. ^ *"Rise of the 'consumer enterprise'". 24 June 2013.*
8. ^ *Lisa Ellis; Jeffrey Saret; Peter Weed (2012). "BYOD: From company-issued to employee-owned devices".*
9. ^ *"BlackBerry Strategizes For More U.S. Government Clients". 2013-01-07.*
10. ^ *"Support BYOD and a smarter workforce".*
11. ^ *"Cisco Study: IT Saying Yes To BYOD".*
12. ^ *El Ajou, Nadeen (24 September 2012). "Bring Your Own Device trend is ICT industry's hottest talking point at GITEX Technology Week". Forward-edge.net. Retrieved 26 September 2012.*
13. ^ *"BYOD research findings". Logicalis. Retrieved 12 February 2013.*
14. ^ *UC Strategies (May 1, 2013). "BYOD's Productivity Gains Are "Hard to Calculate" – Study Says". Retrieved July 11, 2014.*
15. ^ *Gina Smith (February 16, 2012). "10 myths of BYOD in the enterprise". TechRepublic.*
16. ^ *"Cisco ASA + Workspot = BYOD". Workspot. Archived from the original on 2014-07-14.*
17. ^ *Bernice Hurst (August 6, 2012). "Happiness Is ... Bringing Your Own Computer Devices to Work". RetailWire.*

18. ^ *Kevin Casey (November 19, 2012). "Risks Your BYOD Policy Must Address". InformationWeek. Retrieved June 19, 2013.*
19. ^ *"90% American workers use their own smartphones for work".*
20. ^ *"What is bring your own device?".*
21. ^ *"Threat, Violation and Consumerization Impact" (PDF). forescout.com.*
22. ^ *"Bring your own device (BYOD) policies" (PDF). Fraud Advisory Panel. 23 June 2014. Retrieved 23 June 2014.*
23. ^ *"The Rise and Risk of BYOD - Druva". 22 September 2014.*
24. ^ The U.S. Air Force Research Lab's (AFRL) Leader iPad Pilot did uses this method to provide its researchers unfiltered access to the Internet, reserving its filtered, sensitive network for other use.
25. ^ *"Nearly half of firms supporting BYOD report data breaches".*
26. ^ 4 Steps to Securing Mobile Devices and Apps in the Workplace - eSecurityPlanet.com
27. ^ *Wiech, Dean. "The Benefits And Risks Of BYOD". Manufacturing Business Technology. Retrieved 28 January 2013.*
28. ^ *"Greatest Threat to Enterprise Mobility: Employee's Children". 2013-05-17. Archived from the original on 2013-08-22.*
29. ^ *"Bring your own device: Security and risk considerations for your mobile device program" (PDF). September 2013.*
30. ^ *"Enterprise & Gateway Suites - Trend Micro". Trend Micro.*
31. ^ *"Implementing BYOD Plans: Are You Letting Malware In?" (PDF). Retrieved August 26, 2017.*
32. ^ David Weldon, FierceMobileIT. "No one-size-fits-all solution for BYOD policies, panel reveals." May 13, 2014. Retrieved Jul 11, 2014.
33. ^ Tom Kaneshige, CIO. "Attack of the BYOD-Killing MDM Software." February 4, 2014. Retrieved Jul 15, 2014.
34. ^ Lauren Weber, Wall Street Journal. "BYOD? Leaving a Job Can Mean Losing Pictures of Grandma." January 21, 2014. Retrieved Jul 15, 2014.
35. ^ *Kaneshige, Tom. "BYOD's Phone Number Problem".*
36. ^ *"BYOD Policy". Logicalis. Retrieved 12 February 2013.*
37. ^ ***a b*** Kenneth C. Laudon, Jane P. Laudon, "Management of

Information Systems"

38. ^ *Jarrett, Marshall. "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations" (PDF). Office of Legal Education. Retrieved 15 May 2013.*
39. ^ *"Marine Corps mobile device strategy looks to cut costs -- Defense Systems". Defense Systems.*
40. ^ *"Oregon.gov: Home". www.oregon.gov. Retrieved 2016-07-07.*
41. ^ ***a b*** *Hassell, Jonathan. "7 Tips for Establishing a Successful BYOD Policy". CIO. Retrieved 2017-02-25.*
42. ^ *Emery, Scott (2012). "Factors for Consideration when Developing a Bring Your Own Device (BYOD)" (PDF). University of Oregon Interdisciplinary Studies Program presentation.*