GlobalLogic®

Bring Your Own Device

by Seema Joshi, Arun Kumar, and Somya Srivastav

Contents

What Is Bring Your Own Device?	1
The Evolution of BYOD	2
What Do We Need for BYOD?	3
BYOD Scheme Components	4
What Are the Potential Risks of BYOD?	7
Real-world Solutions for BYOD	9
The Future of BYOD Security	10

What is Bring Your Own Device (BYOD)?

BYOD stands for Bring Your Own Device, a work culture shift where an organization's employees can use their personal devices for work purposes.

Participating organizations do not compel their employees to use devices provided by the company. Instead, they leverage their employees' personal devices and access the organization's private network, mail, and file-sharing systems.

Personal devices could be laptops, smartphones, hard drives, or any other form of information technology.

"The employee is allowed to access work apps, mail, file sharing, and other privileged information not only on their laptops but also on their mobile phones."

Why is BYOD Important?

Employees working in an organization where they are provided with a dedicated or floating device can only work on that device. Most of the time, employees also have their personal devices with them, but they cannot use them for work purposes. They have to juggle two devices for personal and professional activities.

Employees who are permitted to use their personal devices for work purposes are more efficient. They also appreciate the freedom to pivot between work and personal activities using a single device.

The use of mobile devices in today's workforce is as ubiquitous as smartphones themselves. Mobile phones grant us tremendous communication opportunities, from voice calls to instant messaging and even video conferences.

Email is also readily accessible on the go. Organizations that allow BYOD will see quicker communication and increased productivity. Workers find it easiest to reach for their personal phones in case of urgent calls or messages instead of managing two devices at a time.

The Evolution of BYOD

Empowering users

Employees feel empowered when they can get things done with a touch on their personal smartphones. BYOD has proven to increase productivity and motivation.

Cost-effective

Organizations that provide their employees with devices have to struggle with extending patches to the devices to keep them secure at all times.

More devices have to be purchased and managed as a workforce expands, which incurs a considerable cost. To save money, many organizations rely on the personal devices owned by their employees.

Working remotely during the pandemic

During the COVID-19 pandemic, most employees, especially in the IT sector, have been working remotely.

Organizations that take advantage of their employees' personal devices certainly have the edge over their competitors. Businesses where employees work on company-owned devices that cannot be carried out of the workplace find it difficult to run their operations smoothly.

Companies with a BYOD culture allow their employees to upgrade their existing personal computer to continue their work uninterrupted.

What Do We Need for BYOD?

BYOD scheme

The BYOD scheme encapsulates all employee privileges and restrictions, without compromising their freedom to use their personal devices. It keeps a record of the various types of personal devices that will be allowed for work purposes. It must contain contingency plans for lowering risk in the event of a security breach.

The company stakeholders must always be considered so the organization understands the scheme's pros and cons.

Endpoint management strategy

To keep the organization safe from any cyber attacks, the employees' personal devices must be regularly monitored. This will help the IT team distinguish safe devices from unsecured ones.

If a personal device is suspected of causing any threat, the employee will have to rely on a company-owned device.

Secure user experience

Organizations with BYOD must provide their employees with a secure user experience, even if they are working on a personal device while connected to a workplace network.

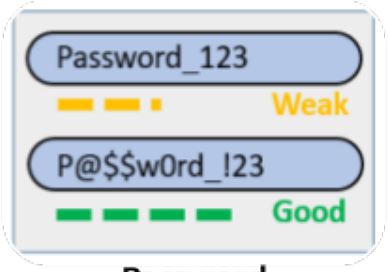
Employees should not need to struggle while accessing company data, apps, and other portals. It's best to simplify the way employees connect to the company's secured assets. The scheme is intended to effortlessly manage all such devices and access requests to guarded assets.

Protected corporate network

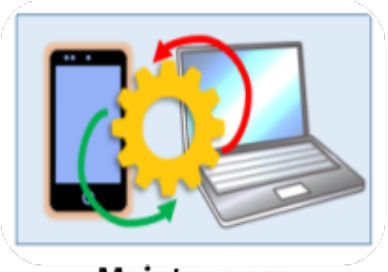
The BYOD scheme should have provisions to protect the corporate environment in the event a personal device is suspected of causing harm.

The scheme should prevent the loss and theft of confidential information and provide directives for risk management. Activities should be monitored while accessing a company's sensitive data.

BYOD Scheme Components



Password Strength



Maintenance Responibility

Prohibit the use of Camera

No Privacy Expectation

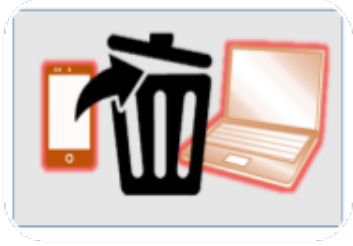
Control on Data Transfer

Encryption of Data

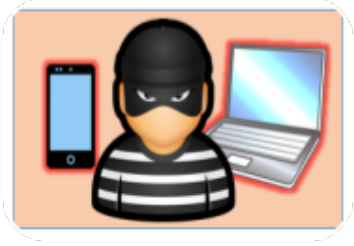
Device Provisioning

Inspection policy when employee leaves company

Management software installation



Data wiping in case of threat



Report Loss or Theft of devices

Failure to follow the scheme

Password strength

A company should establish rules for setting up passwords using alphanumeric and special characters. The IT department should lock a device in the event of multiple failed attempts to log on to a device.

Maintenance responsibility

The maintenance of personal devices must be the sole responsibility of the employee. The company may reimburse expenses or can appoint third-party providers for maintenance.

Prohibit camera use

Smartphones today have a camera feature, but most companies or stakeholders do not allow employees to take pictures in the workplace or capture images on work screens.

No privacy expectation

Companies often keep close track of their employees, monitoring everything from personal activities to phone calls. Organizations will often limit employee privacy to reduce possible future litigation.

Control of data transfer

The BYOD scheme should impose a ban on transferring any corporate data to or from outside the secure corporate network. This prevents any unauthorized transaction of information and safeguards the company's data.

Encryption of data

According to company policies, all data transfers must be encrypted in order to prevent any attackers to breach in and steal sensitive information. Encryption is the pillar of the BYOD schemes laid down by the companies.

Device provisioning

All employees who use personal devices first need to have their devices provisioned by their company's IT department. This ensures that the devices are correctly configured and prepped with security protection to counter any cyber attackers.

Inspection policy when an employee leaves a company

When an employee leaves a company, it is necessary to inspect their personal device. Usually, the IT department checks for any sensitive corporate data that the employee may carry forward after their exit. This check may be optional, and the employee's manager should direct it.

Management software installation

Companies providing a BYOD scheme often deploy their own applications on personal devices to manage or secure work activities. Such apps can be mobile device management, endpoint management, or anti-virus software.

Data wiping in case of threat

Companies can deploy applications on personal devices that lock the device after multiple failed attempts to unlock the device. The app can also delete all sensitive data to prevent theft.

Report device loss or theft

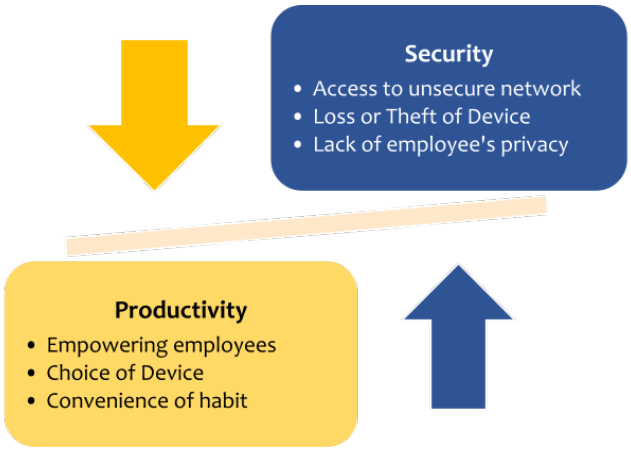
If an employee loses their device or it is stolen, the employee must immediately report the incident to the company's IT department. This will help the authorized body wipe out or lock the device to protect the company's sensitive information that may have been saved on the device.

Failure to follow the scheme

The scheme must clearly highlight the consequences of failure to abide by the BYOD rules by the employees. A strict punishment must be announced in case of failure to follow the scheme. The punishment rights are reserved with the company and may range from depriving connection privileges from the corporate network to termination of the employee.

What Are the Potential Risks of BYOD?

While BYOD is employee-friendly, it may prove to be more threatening than comforting. An organization's secure corporate network, mail, file sharing, and other portals will face potential risks when employees use their personal devices to gain access.



Personal smartphones used under a BYOD scheme can be carried to social gatherings, while commuting and shopping, and many more places. There is a high risk that they will be lost or stolen at some point because they can be taken anywhere.

Once a device is out of an employee's hands, we can never know what confidential information has been compromised.

Opportunities for data theft

Employees working under BYOD are easy targets for hackers. Whenever a user connects to an unsecured network with their personal device, a cyber attacker has the opportunity to break into the corporate network and steal sensitive information for malicious purposes.

Malware infiltration

Although employees will attempt to adhere to BYOD guidelines, they may not be careful to segregate personal data and apps from work-related ones. Any malware that reaches the device through any personal apps can compromise any corporate information stored on the device.

Potential legal issues

While BYOD gives employees freedom, it may also land the company in legal trouble if there is a breach in security and sensitive information is lost. The organization may face legal action as per the agreement between a company and its stakeholders, who can be implicated and may hold the company accountable.

Loss or theft of device

Most employees use their smartphones for work under the BYOD rule. If a device is stolen or lost, the company may have problems if the employee did not follow the BYOD scheme.

Lack of training

More and more quality training for the employees using their own devices be it laptops or mobile phones will ensure that the employees are more watchful of any potential security break-ins and will contribute to keeping up the security walls intact.

Shadow IT

Shadow IT is the use of IT infrastructure such as software or hardware without the knowledge of a company's IT department or security group. As cloud-based services have become the next big thing, concerns have arisen about unauthorized usage to meet demands and deadlines.

Employee privacy

There is a trade-off between employee privacy and organizational security. As a company imposes security restrictions on personal devices, employee privacy is bound to be hindered. Though BYOD practices increase productivity, it compromises privacy. BYOD schemes are normally prepared with little flexibility for employees.

Lack of uniformity

All employees will not use the same type of device. Some may use iPhones or Mac, and others will prefer PC or Android. In a team of 10 people, six may use Dell, and four may use Macs. Operating issues are likely to arise. It may also require IT people to learn two different operating procedures, as well as other complications. It will be more efficient for the IT department if everyone uses the same devices, but businesses may need to pay for them.

Liability

When an employee uses a device for work and personal life, who is liable for repair or replacement costs? It must be clearly established who will pay these expenses if something happens during work hours. These are questions that need to be carefully considered and answered before implementing a BYOD program in your organization.

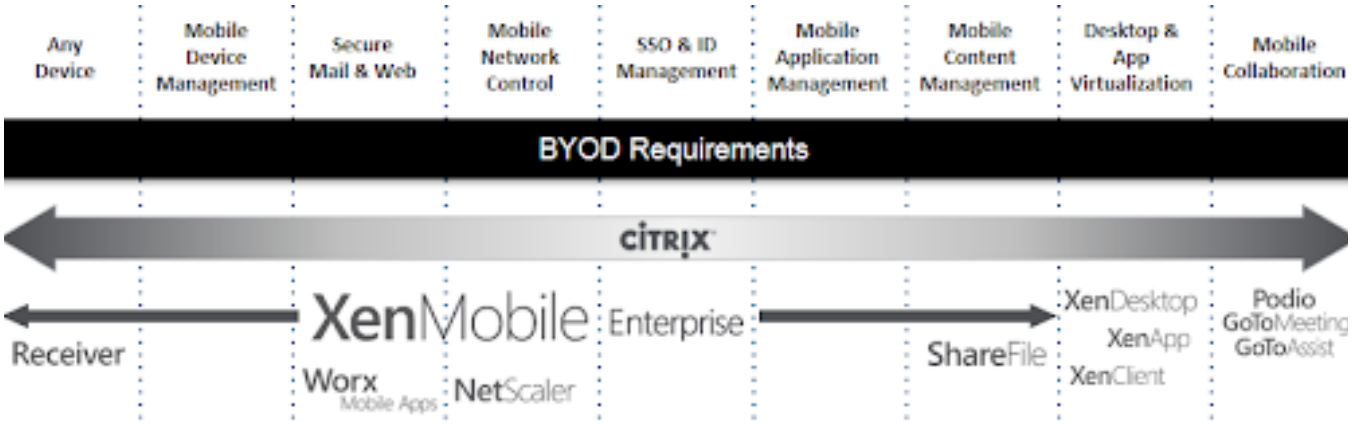
Data retrieval

When an employee leaves the company, it may be necessary to remove the organization's private information from the employee's device, which could prove to be difficult. A plan should be in place to prevent the potential misuse of information. All of the risks discussed above are of extreme concern but they can be planned and be prepared to fight against it. Any threat, if identified well in time can be mitigated, provided that the organization must have a well-devised BYOD scheme.

Real-world Solutions for BYOD

BYOD requires businesses to develop solution products that allow users to access the company's data, mail, internet, and other infrastructure. Users will need to set up this product or application on their personal devices. Such products assist an organization's IT department in maintaining security enforcements as described in the BYOD scheme. The IT team can efficiently control employee activities that may breach security protocols.

Citrix is one company that is practicing BYOD through its solution product.
Citrix offers desktop and app virtualization for any device. It caters to mobile device management, secure internet and email, mobile network control, ID management, and mobile app and content management.



Desktop Virtualization

Probably one of the easiest ways to get started with the BYOD is desktop virtualization. A user can access an isolated logical operating system instance from a personal device without installing any programs.

VM Horizon Client is another such solution product, developed by VMware, Inc.

This software also enables remote access to the workplace through desktop virtualization. It separates the desktop environment and VMware's application,and runs across work platforms.

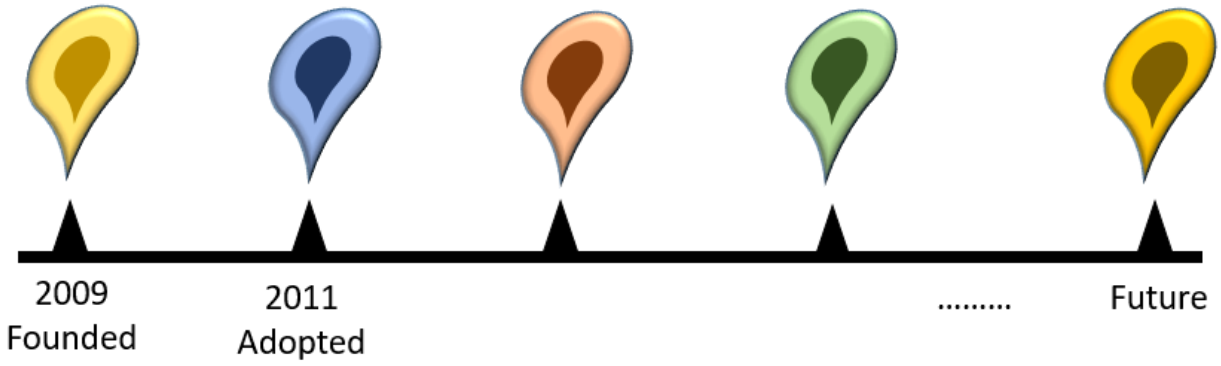
The Future of BYOD Security

A BYOD scheme works well when it is intelligently drafted by the organization and genuinely followed by its employees. There are also solution products that manage all cross-platform devices in use, yet we see a lot of scope for improvement in the security aspect of this ensemble.

In the future, we look forward to solutions to the gaps between users and work environments. Such solutions will be administered under the respective BYOD schemes drafted by the organization.

They will benefit from increased employee productivity that comes from using personal devices combined with the IT infrastructure offered by the corporate environment. Future solutions will be able to deal with security risks and make sure personal data is not compromised.

The IT team in this scenario will play the crucial role of handling any breaches detected and patching workstations regularly.



References

Hollander, Garrett. “The Top 7 Risks Involved With Bring Your Own Device (BYOD).” M-Files, 24 March 2019, https://resources.m-files.com/blog/the-top-7-risks-involved-with-bring-your-own-device-byod-3. Accessed 12 March 2021.

“What is BYOD (Bring Your Own Device).” citrix.com, https://www.citrix.com/en-in/glossary/byod.html. Accessed 12 March 2021.

“What is Shadow IT.” Cisco.com, https://www.cisco.com/c/en/us/products/security/what-is-shadow-it.html. Accessed 12 March 2021.

About the Authors

Seema Joshi is senior technical manager with GlobalLogic, having diverse expertise in development and running mostly digital transformation projects in versatile domains.

Arun Kumar is a QA Lead with GlobalLogic, contributing in various streams through his automation as well as manual testing skills.

Somya Srivastav is an enthusiastic developer working in financial projects utilizing her .NET skills.

GlobalLogic®

GlobalLogic is a leader in digital product engineering. We help our clients design and build innovative products, platforms, and digital experiences for the modern world. By integrating strategic design, complex engineering, and vertical industry expertise,— we help our clients imagine what's possible and accelerate their transition into tomorrow's digital businesses. Headquartered in Silicon Valley, GlobalLogic operates design studios and engineering centers around the world, extending our deep expertise to customers in the communications, automotive, healthcare, technology, media and entertainment, manufacturing, and semiconductor industries.



www.globallogic.com