BYOD

EBOOK BY TEAMSID

BYOD

BRING YOUR OWN DEVICE STRUCTURES

*As of 2015, **36%** of companies have implemented some form of BYOD policy. By this year, it is estimated that more than **50%** will have made the move and **74%** have either done so or are considering a transition. That's an increase of **50%** over that time period, and it's projected to continue increasing rapidly in the coming years.*

Companies are flocking to what would have been considered horrible policy only 15 years ago, in part because of the nature of the apps we use and the way we consume data. 95% of businesses have at least some of their business-critical apps hosted in a public or private cloud, and those applications offer secure access to vital data anywhere with an Internet connection.

Rather than supplying employees with expensive smart phones, tablets, and laptop computers, companies see the opportunity to reduce their IT infrastructure spend and focus on applications, security, and management – which in many ways can be both more secure and less expensive for the company.

Financial industry employees are more likely to use their own devices and the numbers are only growing.

In addition to the major industries, there has been an increase in the number of remote workers. While contractors are certainly most likely to use their own devices, there are a growing number of businesses seeking to expand the pool of employable talent by hiring remotely and not requiring staff to meet in the office. For these companies, BYOD is a necessity, not an option, making it even more important to have a clear policy in place.

The shift from banning cell phones at work to encouraging their use both in and out of the office to expand the work day started several years ago, and is borne out in the data.

More than half of people surveyed are using their smart phone or tablet at work, and a growing number are using their own laptop computer both in the office and on the road.

In terms of industry, there are some that embrace the model more than others. Those that travel frequently, work extended hours, or encourage round the clock availability are more likely to utilize BYOD than others.

BYOD

BENEFITS

Why are so many companies shifting to a BYOD model for their employees? What benefits are they getting from allowing employees to bring in previously undesirable distractions to the workplace? There are quite a few, it turns out, and as more studies are done, it has become apparent that having at least a partial BYOD policy makes sense for almost all business types and sizes.

1. PRODUCTIVITY & EMPLOYEE SATISFACTION

One of the primary reasons companies allow employees to use their own devices is the productivity boost it frequently brings.

The ability to work anywhere and at any time, not just when in the office, is a huge boon – opening 70% of the week to additional work potential, and allowing more engaged interaction during travel. It also allows for a more flexible work from home policy, sick days and vacation are less taxing on the company, and employees don't feel walled off from the outside world while at work.

2. TALENT ATTRACTION & RETENTION

Because of the increase in employee satisfaction, and because BYOD makes remote work much more feasible, it's easier to attract and retain top tier talent.

American mobility is at a decades-long low. People are moving less and jobs are getting harder to fill. By opening your hiring and work policy up to be more flexible and allow for remote opportunities, you vastly increase the size of your talent pool.

BYOD

BENEFITS

3. LOWER IT/SUPPORT COSTS

IT and support costs are reduced almost immediately because your company isn't immediately responsible for managing multiple devices per employee.

While day to day support is still a necessity, the heavy cost and time dedication needed to manage hundreds of desktops, laptops and mobile devices can be greatly reduced.

.

4. COLLABORATION

A BYOD policy opens new collaboration opportunities between staff. Imagine the ability to quickly coordinate with staff while in a client meeting or to ask for a file from your phone at the airport. These are near impossible when working from company-issued equipment, especially if they don't provide mobile devices.

At the same time, the use of cloud apps makes it possible to access and work with files from on the go just about anywhere, greatly increasing collaboration opportunities.

5. BETTER CARE & LONGEVITY IN DEVICES

One of the reasons so much time and money is spent in maintaining corporate devices is that employees have little reason to be careful with them. Whether it's leaving on a desktop for weeks at a time or tossing a company phone into a backpack, it's not theirs, so the general care that goes with most technology isn't there.

That changes when employees use their own devices. They are more careful in general and the devices you do purchase last longer as a result.

BYOD

CHALLENGES

With so many clear benefits, it's no wonder that more than half of all businesses have latched on to the idea, and why so many startups are by default encouraging staff to use their own machines.

But it's those companies that don't think about the ramifications or that do it out of necessity without considering the alternative that are at the greatest risk of problems.

There are many logistical challenges and security risks that can ultimately make a BYOD policy into an issue if they aren't dealt with early and managed over time. These include:

1. DATA PROTECTION

When company information leaves the office on a personal device, risk increases significantly. People use public WiFi, have their devices stolen, or lose them when out of the house, and if your vital information is on that device when it's lost, it can be a major problem.

2. SECURITY

The firewall, antivirus, and security update work you do on local machines is meaningless if your employees download client data and never update their own devices.

Access control for critical data is very important for this reason, as is the ability to followup and check on the current status of devices that are connected to the company network.

BYOD

CHALLENGES

3. SUPPORT

If an employee has problems with a cloud application or software and data for their job, how do you handle support. Where is the line between IT support for company devices and BYOD support to ensure they can continue working at peak efficiency?

When a company-owned laptop breaks, it goes to IT and gets repaired as quickly as possible, often replaced by a loaner in the meantime. If a personal laptop breaks, it might be days or weeks before the employee can get it fixed or afford to replace it. This can mean lost productivity if there isn't a backup option available.

4. COMPLIANCE & ADHERENCE

It's easy to track activity on a local device, whether with admin-level tracking software or firewalls that block unwanted activity. But it's not as easy to stop an employee from surfing Facebook, downloading movies, or otherwise misusing their own personal devices.

Compliance with the security protocols put in place is vital to avoid major issues in the future, but so too is adherence to the basic rules for accessing and using data in the workplace.

BYOD

SECURITY PROVISIONS

To address the common challenges faced by companies with a new BYOD policy, it's important to have certain security provisions in place. Properly implemented, these will ensure that there are no major issues that can put sensitive employee or customer data at risk.

For industries in which data is sensitive or protected, this is even more important because of the potential liability it represents for your company. Some of the things you should keep in mind when building a bring your own device policy include:

1. VIRTUALIZATION

Even with security certificates and installations on employee devices, the frequency with which users upgrade their devices makes it difficult to fully control access and security on those devices.

Virtualization on mobile devices and personal laptops makes it easier to control access to vital company information, locking apps, desktop access, and company data behind a virtualized instance on their device. Software like VMware allows for a virtualized desktop experience that gives the freedom of BYOD and the security of in-house equipment.

2. CONTAINERIZATION

With the risk of data leakage on most devices as high as 80%, containerization is an effective solution. Containerization allows for locking down app-specific data, and some solutions will encrypt inter-app communications, protecting user credentials and configuration details. This encryption needs to be device independent to ensure consistency across all user devices without impacting user experience.

SECURITY PROVISIONS

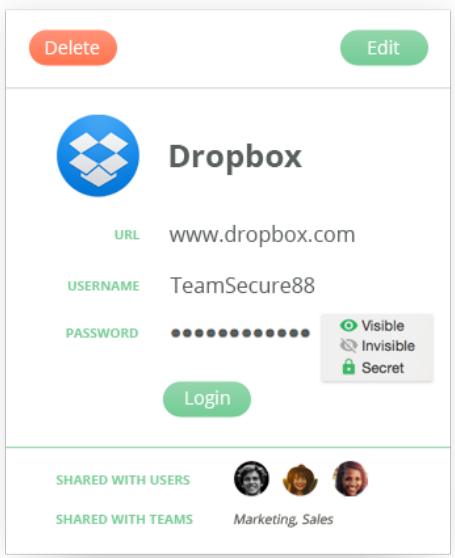
3. POLICY & COMPLIANCE GUIDELINES

The technology is important, but so too is the policy governing how it will be used. Your staff needs to know what is appropriate, how they are supposed to access company data, and what precautions need to be taken if they do utilize personal devices for business.

A simple and easy way to secure your company's web logins and passwords from BYOD security vulnerabilities is to use a business password manager. Try our TeamsID business password manager FREE for 14 days!

TeamsID is available on any the all devices your employees could be bringing to your office.

Mac App | Windows App | Android App | Apple iOs App | Chrome Extension



BUILDING A STRONG POLICY FRAMEWORK
NEXT PAGE >>>

BYOD

BUILDING A STRONG POLICY FRAMEWORK

To ensure compliance from your staff, you need a strong policy in place that clearly outlines what is and is not allowed. Simply saying "yeah, you can bring your tablet to work" isn't enough. It needs to be clear what the expectations are for all devices connecting to your company's network, and how data will be secured and handled on those devices.

---

*There are two major areas for which policy needs to be defined, including **devices** and **users.***

BYOD

BUILDING A STRONG POLICY FRAMEWORK

DEVICES

For devices that will be used by staff, there are several factors that need to be considered and for which policy needs to be established, including:

SCALABILITY	If you implement a virtualization or containerization solution, make sure it is scalable for your team as it grows. Smaller scale solutions like password management can be a good way to start, especially if you aren't working with critical client data.
CRITERIA	Which devices are allowed, what specifications must they meet and what is eligible for access?
CONFIGURATIONS	Specific apps, security setups, and device specifications should be mapped out in advance for employees. Platform preference is also important.
SUPPORT	Make it clear what responsibility the company has for support and how it will be managed if a problem occurs.
SECURITY	Determine the security protocols that will be used to protect login access, lost or stolen devices, wireless connections, and passwords.

By having a clear plan in place for each of these, you can avoid outdated devices without any security measures in place accessing your sensitive company data.

BYOD

BUILDING A STRONG POLICY FRAMEWORK

USERS

Beyond the device policy, you should have clear guidelines in place for the individuals who are allowed to bring devices to work, and what their use can entail. Factors to consider include:

ELIGIBILITY	Will all employees be eligible or will BYOD be specific to certain departments or employees? Is training or certification required?
USAGE	What will personal devices be able to access and how can they access it? You may decide that certain on-premise applications are only accessible through company devices.
COMPLIANCE	How will compliance be measured and maintained. Will you perform regular audits to ensure access rules are being followed?
LIABILITY	From a legal perspective, how will you handle liability for devices brought in by employees. Speak with your legal team in conjunction with security staff to ensure this is covered.
REIMBURSEMENT	What kind of reimbursement will employees be offered, if any, for use of personal devices for work purposes, especially if travel is involved.
VIOLATION POLICY	What happens if someone violates the policies you have set? Will they lose their BYOD privileges?

With these factors all clearly defined, it becomes easier to not only trust your staff to follow your policies and protect company data, but to allow an ongoing policy as your company grows.

BYOD

TRANSITIONING TO A BYOD WORKPLACE

The transition from company-owned and managed hardware to a BYOD-friendly workplace should be gradual and carefully managed. Clear guidelines of who is allowed to take advantage of this policy and how they are expected to do so will ensure a smooth transition and a more secure workplace for your data.

Training and security guidelines should be updated frequently and there should be an administrator whose role it is to oversee all such policies, ensuring that no future security holes develop.

To learn more about what you can do to make BYOD more secure without introducing undue burdens to your staff, consider TeamsID. A simple, easy-to-use password manager that allows you to control access from a central dashboard, TeamsID encourages collaboration and productivity without the risk of lost data.