A (SURPRISINGLY PAINLESS) GUIDE TO

B.Y.O.D

D-Link®
FOR BUSINESS

TABLE OF CONTENTS

INTRODUCTION

Without the right foresight and planning, a Bring Your Own Device (BYOD) program can turn into a messy project that burdens IT departments.

Instead of providing an easy way for your company's employees to access files (and stream movies from their mobile devices), poorly executed BYOD initiatives create a heap of IT helpdesk tickets and disgruntled employees.

It's part of the reason why just a few years ago nearly half of all companies were banning the practice of BYOD programs.[1] That, and constant security concerns over breaches, malware, ransomware, and hacking.

Things have changed since then, though. Nearly 60 percent of companies have a BYOD plan[3] in place today. Those companies are reaping the benefits, too.

Here are just a few of them:

- Employees at companies with BYOD programs save an average of 58 minutes each day and are 34 percent more productive.[2]
- BYOD programs can save companies up to $1,350 per employee.[4]
- Employee devices are often more modern, and sometimes more powerful, than company devices.
- Newer devices help prevent the nearly $2 billion companies lose each year[6] in lost productivity due to outdated and obsolete technology.

Not only can a properly implemented BYOD program save you time and money, it can also help you improve security measures. One of the main reasons companies are hacked or suffer data breaches is because they're still using outdated systems with weakened security.[5]

That doesn't mean simply adding a BYOD measure to your company will help. They have to be secure to provide added security. Smartphones are one of the most attacked and vulnerable pieces of mobile tech—and they're the ones your company's employees will use the most.[9]

Now, with that said, there is a way to develop a strong BYOD program and we're going to help you with it from start to finish. When you're all done, you should have a policy in place that will help you provide more security, allow your employees to take advantage of their mobile devices, and help your company meet its long-term goals.

It might even make you look like a bigger genius than you already are.

Here's what we're going to do to meet this goal:

DEVELOP THE PLAN • **DISCUSS THE PLAN** • **CHOOSE THE PLAN**

STEP 1 - DEVELOP THE PLAN

CREATE (THE FIRST DRAFT OF) YOUR BYOD POLICY

When you create a BYOD initiative, you need to think of it as both a part of your network and an extension of it. Many of the policies and regulations that already govern the devices within your company will also apply to the mobile devices your employees use.

This includes what they use the network for, which files and content they can access, and who information and data can and can't be shared with.

For the most part, this is a great thing. It enables your staff to work remotely and have access to tools that can help them be more productive.

Unfortunately, it also means there will be more opportunities for those with malicious intent to steal or hack your company's devices and access confidential data.

That's why the first step in developing a BYOD program is to create a plan.

Here's what you need to plan for:

COMPLIANCE AND REGULATORY MEASURES

Before you give your employees the ability to access confidential company information from the comfort of their favorite coffee shop, make sure you have a strong understanding of all the regulatory measures you need to meet in order to maintain compliance.

Opening up your network to mobile devices may increase the number of local, regional, and national regulations your company now falls under. It's important you understand this well enough to be able to communicate it to the company.

Once you have that squared away, devise action plans on the off chance someone from your company ever breaks them or a breach is discovered.

Even with these plans in place, you might not be able to stop every potential breach of policy. But you will have a better chance of preventing a lost phone from turning into a multi-million-dollar data breach.

SECURITY AND CONTROL

Ever since there have been rules, there have been people trying to find ways around them.

Whether you want to admit it or not, the employees at your company are no different. In fact, 95 percent of companies have reported at least one attempt by employees to override their security measures.[7]

This includes actions such as jailbreaking devices to bypass root permissions on Android, iOS, and other mobile operating systems, and trying to remove corporate management software from the device. (More on this in a little bit.)

When something happens, not if, you'll need to be prepared. This includes having an internal action plan and a set of disciplinary actions your employees should be aware of before they use their own devices.

This can include something simple such as software that automatically quarantines devices until all security criteria have been met, disciplinary action, an investigative protocol, and more.

Most of the time, jailbreaking or software removal is attempted for non-malicious reasons. (Sometimes it's because you just need a break and a short mobile gaming session from the bathroom does the trick.)

But it does happen, and that's the problem.

Malware and other malicious attacks prey on outdated and less secure apps, devices, and weak passwords. Your corporate files contain valuable and, more importantly, private and personal information about employees.

HR Systems files are some of the most sought after data from companies. One profile or folder of someone's personal data alone can sell for as much as $50 on the dark web.[8]

So, before you give your employees the opportunity to use their devices for work, you should inform them of the importance of security and compliance. Then, you should plan for the inevitable.

APP ACCESS

As we just mentioned, apps are vulnerable points of entry, and you'll need to determine which ones can be used on employee devices and how you'll monitor them.

Some of this may be determined by what you need to do to ensure compliance. Not all apps will meet the security standards or regulations you have to maintain. Beyond that, the rest is up to you and open to discussion. (More on that in Step 2.)

While you plan this, here are some factors you should consider.

YOUR SECURITY POLICY

If you plan to restrict usage to company-approved applications only, it could make it challenging for those using older devices as they might not be able to handle newer apps.

However, if you allow people to pick and choose the apps they use, it could be a challenge to maintain performance across your network.

APP SECURITY

It will be easier for you to ensure app compatibility, security, and compliance if you only allow company-approved apps. But you risk limiting what your employees can do.

After all, while Facebook might be an eight-hour rabbit hole of lost productivity for some people, your social media manager might need the app to stay on top of posts and comments on your company pages.

NEW APPS

Your employees are always searching for new apps to help them do their jobs. If they find a new one, how will you handle new apps your employees want to use? Will you allow them to add them as needed? Submit them for review? Perform quarterly or yearly reviews?

Some companies choose to employ a blacklist while others prefer to whitelist them as they come up. Ultimately, it will depend on how much time your IT department has to devote to managing this process.

If the blocking of apps limits the checking of email, calendars, contacts, and the access of Wi-Fi networks and VPNs, you might want to reconsider whether you're headed in the right direction.

USER PRIVACY

Privacy has always been a hot topic, but it's burning a little hotter recently with reports of how companies handle both public and private data. In some cases, there are privacy laws that prevent you from collecting any information on employees at all.

When it comes to collecting employee data, our recommendation is that you avoid it unless absolutely necessary.

If you have to, though, you should limit the amount you collect, including personal emails, contact information, calendars, device location, personal photos, app data, text messages, voicemail, and call history. Even if the data does directly relate to your business.

On the other hand, corporate materials, files, apps, and other items should be—and must be—protected by a company. Containers can help you separate personal and company data while keeping it private and make it easier to remotely wipe devices if needed.
For example, if an employee loses their phone while traveling and a ridesharing app on the device contains company credit card information.

Whether you decide to collect data or not, your employees will need to know. If you do choose to collect data, they'll need to know what you're collecting, what you're using it for, and whether or not they can see what's being collected on them.

It is worth mentioning though, that collecting data could scare your employees away from enrolling mobile devices, limiting whether you can collect data at all.[10]

Basically, what we're trying to say is choosing whether or not to collect data is a tight-rope walk between angering everyone at your company and, well, angering everyone at your company.

Tread lightly.

MOBILE DATA COSTS

When your company's employees work remotely, either because they're remote workers or because everyone wants them out of the office, they might find themselves depending on mobile data.

The question then becomes: Who's footing the bill? Some companies open up their wallets and pay for all the mobile data that's needed. Others set limits. Some answer the question with a firm, "No."

No matter which answer you decide to give, you should create a policy that informs your employees of what's covered and how. Some of this can be done through your BYOD software. (More on that later.)

PERMISSION

Once you have all of the finer details of your program set up, you still have to go through the enrollment process.

One way or another, you need people to agree to your company's terms and conditions in order to use it.Many companies do this through management software. After (pretending) to read all of the small print, employees can click accept, download some software, and begin adding their mobile devices.

Other companies prefer the tried and true method of printing out a ten-pound pile of contractual paperwork and having an employee sign on the dotted line.

With enrollment through software, you have more control over the level of security employees must maintain in order to use your network. This will give you more control over the devices that are allowed on the network.

STEP 2 - DISCUSS THE PLAN

No matter how much planning you do, and no matter how many scenarios you prepare for, there will always be something you haven't considered.

Which is why you need to run your plan through a gauntlet of company employees.

You can do this a few ways, including a mandatory meeting (that people will try to avoid), a survey (that no one will respond to), or an email (that people won't read).

Since everyone's feedback is important, you might consider incentivizing this step, whether that's through throwing a party, providing gift cards, or giving everyone an extra day off.

When you do this, don't forget anybody, though. From the CEO of the company who's always away (playing golf) on business trips, to the contracted workers who you may hire to fill in the gaps, they're all important.

Use this opportunity to explain your reasons for the BYOD program and all of the policies included in it. Gather information about the devices and apps your employees need and use.

Approach this step with an open mind, though. Allow everyone to ask questions. At this point, there are no dumb questions.

If someone asks, "Will this affect the coffee machine?" you should assume there's a reason. Maybe they use an app to control it. Maybe they're just worried it will stop working.

Or maybe denying them their daily dose of morning go-juice will cause them to destroy your entire IT infrastructure.

Whatever it is, the last thing you want to do is implement a BYOD program that prevents someone from using a device or app that helps them do their job—especially if their job is making sure you get paid.

Take the information you receive from this step, then go back to Step 1 and run through your plan again. You may need to go through a few revisions to solidify everything and make it work for as many people as possible.

If you find that every plan you devise creates more limitations than opportunities, you may need to consider the possibility that a BYOD program isn't for you.

That, or you need to start over again and figure out a new plan.

STEP 3 - CHOOSE THE PLAN

Now that you've finished going through your revisions, you should have a finalized plan in front of you. All that's left is to implement it.

There are a few main options that companies use to implement a BYOD program. The first includes modifying the network infrastructure they currently have in place.

It's an old school method, but it can work if you have the time and know-how.

The other two options are software and hardware.

We're going to talk about the pros and cons of these.

If you've already developed a plan and discussed it with your company, consider everything you discovered as you read this. If you're just reading this for the first time, thinking about how the following might affect your company.

Just know that, even if you like one more than the other, your budget, IT staff, and infrastructure may dictate the route that's best for you anyway.

OPTION 1 - SOFTWARE

Many companies opt to go with Enterprise Mobility Management (EMM) or Mobile Device Management (MDM) software for their BYOD program. Most EMM tools include a form of MDM or Mobile Application Management (MAM) as part of the package.

EMMs help you enroll devices, enforce policies, update apps, and manage access. They also include nifty features such as data usage alerts, device quarantine, user-agreement software, and simplified enrollment procedures.

As people enroll, the management tool requires each person downloads and installs software, plus accept any applicable user agreements, for each device.

Since all of the settings, policies, and apps are contained within the software, which is housed on a server or the cloud, you have more control over the network, its security, and its performance.

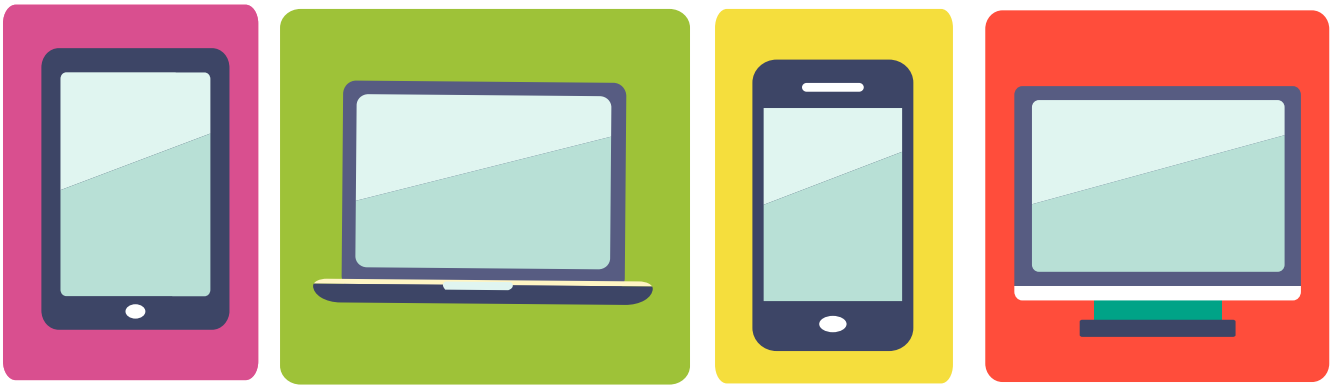
EMM and MDM options make it easier for you to adjust settings for specific apps or a group of apps, including the policies that guide how and when employees can use them.

With software, you can also create separate accounts and login credential for all of the different apps on your network. It's easier to keep sensitive information private and safer this way.

While most software options are easily scalable, they can be costly for smaller organizations. However, they will usually provide a comprehensive list of compatible applications and built-in management tools you won't find through hardware.

Your EMM software suite should:
- Make it easy for employees to sign up
- Reduce, or eliminate, IT helpdesk tickets
- Provide password reset options
- Include lost device location
- Allow remote data wiping
- Deliver a copy of signed BYOD policy agreements, or AUAs, to each employee

Your EMM software suite should give you the ability to share credentials for:
- Wi-Fi Networks
- Email
- Contacts
- Calendars
- Apps
- Shared Drives
- VPNs



OPTION 2 - HARDWARE

Although they won't have all the features that most EMMs have, hardware solutions can provide a more financially feasible option for those wanting to implement a BYOD program.

Most of the BYOD management is performed through a cloud-managed network solution (CMN) using role-based access control, 802.1X, RADIUS servers, two-step authentication, SSIDs, and other adjustable network settings.

You won't be able to set app-specific settings through the CMN, and most of the apps will either be hosted on your server or installed by employees on their devices. But that doesn't mean a CMN solution is less secure than a software-based program.

You can still require employees to accept user-agreements that inform them of what they can and can't do while using your network. Segregated network access through departmental SSIDs and passwords also help you add an extra layer between devices and data.

However, there's not a lot in the way of keeping employees from using any of their devices to access company files. And, if they ever lose their device, there might not be much you can do to remotely wipe them. (Though, if you wanted, you could mix a CMN with an EMM.)

While a CMN doesn't provide all the tools of an EMM, it does provide three benefits that you won't find through software—rapid deployment, predictable and cost-effective scalability, and improved network performance.

Because CMN solutions include switches, access points, and more, you can use them as an opportunity to upgrade your network. This is especially true if an EMM doesn't make sense for your organization, but you still want to implement a BYOD program.

If anything, you could use this as an opportunity to refresh your network, gutting out old switches nearing the end of their life and APs using older, less secure wireless standards.

Solutions with rapid deployment, or zero-touch deployment, also make it simple to add bandwidth as needed. Once you install new switches or APs where you need them, they'll automatically download and copy any configuration settings you've set up.

It's a real time saver and may prove more cost-effective than EMM if you ever find yourself adding hundreds or even thousands of mobile devices, such as tablets.

Basically, it's a nice 2-for-1 option where you can justify the cost of adding new technology while hgiving your employees the chance to use their devices at work.

CONCLUSION

Whether or not you want to implement a BYOD program is up to you. There's a lot you need to consider, including security, compliance, and applications.

If you decide the time is now, we can help you—even if all you have right now are questions.

Here's what we can do to help you:

Talk with you to understand your business goals and needs
Perform a site survey
Work with you and a reseller to diagram and plan your network
Send field engineers to help with deployment and configuration, both before and after the installation Provide no-cost support for the lifetime of your products.

REFERENCES

Further Reading:
12 Features That Make Cloud-Managed Networks Easy To Manage

References

1. Hamblen M. The bring-your-own-device fad is fading [Internet]. Computerworld. Computerworld; 2015 [cited 2019Jun12]. Available from: https://www.computerworld.com/article/2948470/the-bring-your-own-device-fad-is-fading.html

2. Employees Say Smartphones Boost Productivity [Internet]. Samsung Business Insights. 2018 [cited 2019Jun12]. Available from: https://insights.samsung.com/2016/08/03/employees-say-smartphones-boost-productivity-by-34-percent-frost-sullivan-research/

3. Bullock L. The Future Of BYOD: Statistics, Predictions And Best Practices To Prep For The Future [Internet]. Forbes. Forbes Magazine; 2019 [cited 2019Jun12]. Available from: https://www.forbes.com/sites/lilachbullock/2019/01/21/the-future-of-byod-statistics-predictions-and-best-practices-to-prep-for-the-future/#61b002f01f30

4. DMS Technology. 3 Big Risks of BYOD [Internet]. DMS Technology. DMS Technology /wp-content/uploads/2016/01/DMS_LogoBlack.png; 2017 [cited 2019Jun12]. Available from: https://www.dmstechnology.com/3-big-risks-of-byod/

5. Dacri B. Thousands of Organizations Run the Majority of their Computers on Outdated Operating Systems, Nearly Tripling Chances of a Data Breach [Internet]. BitSight. [cited 2019Jun12]. Available from: https://www.bitsight.com/press-releases/thousands-organizations-run-majority-of-computers-on-outdated-operating-systems

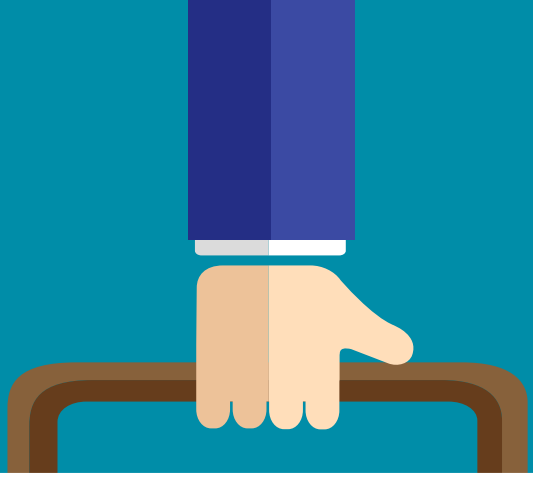
6. bizjournals.com. [cited 2019Jun12]. Available from: https://www.bizjournals.com/phoenix/news/2018/11/15/outdated-technology-costs-businesses-more-than-it.html

7. Bolden-Barrett V. Employees use personal devices for work without much oversight [Internet]. HR Dive. 2018 [cited 2019Jun12]. Available from: https://www.hrdive.com/news/employees-use-personal-devices-for-work-without-much-oversight/523913/

8. Bolden-Barrett V. HRIS, ATS technology is big target of cybertheft [Internet]. HR Dive. 2017 [cited 2019Jun12]. Available from: https://www.hrdive.com/news/hris-ats-technology-is-big-target-of-cybertheft/435599/

9. Ng A. Your smartphones are getting more valuable for hackers [Internet]. CNET. CNET; 2018 [cited 2019Jun12]. Available from: https://www.cnet.com/news/your-smartphones-are-getting-more-valuable-for-hackers/

10. IoT and BYOD Devices Bring Holiday Fear [Internet]. GetApp Lab. 2019 [cited 2019Jun12]. Available from: https://lab.getapp.com/iot-and-byod-devices/



D-Link®

FOR BUSINESS

A (SURPRISINGLY PAINLESS) GUIDE TO B.Y.O.D