# Collaboration Manage360°

CRA's Secure File Sync, Share and Collaboration Solution

## How to Make the Best of BYOD

White Paper

## Introduction

BYOD, or Bring Your Own Device, is a trend that is fast overtaking businesses in every industry. BYOD refers to business practices which allow, encourage, or perhaps even require employees to bring in and use their own personal phone, tablet, or laptop computing devices to perform business tasks in or out of the workplace. Companies that harness the power of BYOD can reap significant benefits. Those that fail to adjust to the trend will be vulnerable to security issues and strategic disadvantage.

The reality today is that most businesses already operate a BYOD environment, whether they realize it or not. The increasing demands in most workplaces for constant communication and expanding hours of expected availability for job tasks means that employees will increasingly be performing work during what used to be personal time and in personal spaces. This combination almost insures that they will attempt to use their own preferred personal computer or mobile device for work purposes at some point.

The trend also runs in the opposite direction, with employees tending to use business devices during work hours to perform personal tasks. Policies and enforcement mechanisms designed to discourage this sort of use, however, also tend to push staff back to their own personal devices. A website-blocking program on their work phone, for example, will just send the employee to their own smartphone, where they can surf freely.

In many cases, those phones may be newer and more powerful than the business-issued option. In any event, employees have already exercised their personal preference in purchasing their individual devices. Corporate purchasing policies, for reasons of cost and support, tend to fixate on a single brand or model, which will assuredly not match the preference of each and every employee. Therefore, some percentage of staff are always going to prefer to work on their own device when possible. Analysts at the Aberdeen Group, an IT research firm, suggest that workers using their own devices experience real productivity gains over workers forced to use business-issued devices.[1]

What these trends add up to is an environment in which some percentage of employees, regardless of official policy or precautions, will find some way to use their own devices for both personal and business use.

1 (Kaneshige, Tom. "Are BYOD Workers More Productive?" CIO. CIO Magazine, 23 Apr. 2012. Web. 22 Mar. 2016.)

"The benefits of BYOD include creating new mobile workforce opportunities, increasing employee satisfaction and reducing or avoiding costs"

-Gartner

## Security

Traditionally, this has been seen as an enormous security threat, and for good reason. Allowing staff to use a wide variety of untested and unmanaged personal devices is a security nightmare for businesses. Without consistent virus-checking, bug-patching, and version control, private devices are ripe for virus infections.[2] And in terms of information security, few personal devices have anywhere near the defenses of corporate networks when it comes to protecting sensitive data. Most users do not engage encryption options on their phones or laptops; a lost device can disappear with millions of sensitive business records, exposing the company to legal issues and public relations nightmares.

The only thing more difficult than coming up with a secure BYOD environment, is preventing those employees from using their own devices in the first place.

This reality is driving more and more companies to formally adopt BYOD policies. According to Tech Pro Research, almost 75% of companies in a 2014 study either permit or plan to permit employees to bring their own devices into the corporate network.[3]

## BYOD Policies

Building an information technology system and a set of policies to support safe, secure BYOD will not only allow employees to use their preferred tools to accomplish their jobs; it can lead to a more efficient, more secure, more predictable technology platform for your company as a whole. Any business with a technology-enabled workforce should strongly consider adopting formal BYOD policies.

A good BYOD policy will force IT administrators and business executives to consider platform vulnerabilities and information access policies in ways that may have been handled in a sloppy and insecure fashion previously. Companies operating completely on what they assume to be a secure internal infrastructure neglect good, layered security and permission practices. All too often, internal networks operate without

2 (Samson, Ted. "Malware Infects 30 Percent of Computers in U.S." InfoWorld. InfoWorld, 8 Aug. 2012. Web. 22 Mar. 2016.)
3 (BYOD Business Strategies: Adoption Plans, Deployment Options, IT Concerns, and Cost Savings. Rep. ZDNet, Feb. 2013. Web. 22 Mar. 2016.)

significant security. The business relies entirely on perimeter defenses to protect valuable systems and data. But this approach leaves a soft underbelly vulnerable to a single bug or lapse in firewall protection.

A network that supports safe BYOD access is forced to address these vulnerabilities. By designing a system that safely controls access from a mixture of employee devices, companies are also building a system that is inherently better protected against directed external threats. For example, your business might currently distribute financial information in individual Excel spreadsheets via email. These are easily hacked, and many copies are made and saved on different devices, making access control almost impossible. But a redesigned system might make the same information available via a securely encrypted remote management application which allows remote wipes and IT-managed access control on any device. This not only provides a secure venue for BYOD uses, but helps secure the internal corporate network as well.

## Cost

IT costs can also be made more predictable and even reduced with smart BYOD policy. Although employees will bristle if forced to purchase all their own devices for business use, almost all of them will accept cost-sharing instead. Since they are allowed to select their own device and to keep it for personal use, a popular BYOD strategy is for the business to offer a stipend to only partially cover the cost. The employee can choose whether to buy something more expensive than the stipend will pay for and many will do so. The business, then, ends up gaining the advantage of more powerful, capable devices than it would if it paid for each of them entirely out-of-pocket.

Offering a regular stipend on either an annual or a biannual basis puts control of upgrades and replacements directly in the hands of the user and takes it off the plate of the business. And since the stipend is a regular and fixed amount, unexpected hardware costs are completely eliminated.

## IT Support

Support is another obstacle in the BYOD universe. IT support staff who might only have had to understand Android devices in the past may suddenly be confronted with an influx of iPhone or Windows Mobile problems. But again, as with security, it can force IT administrators and executives to design support systems and policies that are more flexible and effective than their current practices. The efficiencies realized by creating more robust and less troublesome processes will usually entirely outweigh the additional support intake.

To accomplish this, business IT staff should focus more on creating and improving self-provisioning and ease of access to corporate systems and less on supporting particular devices. Designing a system that is broadly supportive of multiple platforms tends to pay dividends outside of just the BYOD question. For example, internal systems that have been redesigned according to industry best-practices to work equally well for iPhone or Android workers will also allow the business to better integrate with external partners or even directly with customers.

BYOD also allows certain categories of support to be shifted away from the business IT department entirely. Since the business is not providing the hardware, staff will generally deal directly and independently with their provider for hardware and device-related problems. The general variation in skill levels among users can be leveraged to the businesses benefit also. Power users will leap at the chance to address their own issues in their own way, freeing up IT staff to work with less savvy users who might require more assistance. Internal self-support groups can also ease the support burden; for example, the IT department might set up a mailing list or forum for iPhone users, where they can share tips and tricks directly without involving corporate resources.

## Solution

Of course, since productivity can be affected by down-time, even when it's outside the control of the business, it may be wise to partner with a company like CRA, who can manage, support and implement BYOD polices for all employees.

The importance of using solid, tested tools for providing corporate data access to BYOD users cannot be overstated. Toward that end, a cloud-based sharing and synchronization platform, such as CRA's ***Collaboration***$^{Manage360}$ is a must. Secure file synchronization and backup can provide compliance and peace of mind to business executives regardless of the device from which any particular user is accessing the corporate network.

CRA™
Transform IT
Computer Resources of America

**Corporate Headquarters**
64 West 48th Street, New York, NY 10036 – 212-376-4040 – www.consultcra.com – sales@consultcra.com