

Sage Construction and Real Estate

Securely using mobile devices
in the construction industry



Table of Contents

Construction workers are driving inevitable change..... 3

Know your risks when employees support their own BYOD use 3

The BYOD risks..... 4

How to minimize BYOD risk..... 4

How to implement BYOD policies and mobile applications 6

 Step One: Declare immediate and simple BYOD employee ground rules 6

 Step Two: Involve your employees. Get their ideas and input 6

 Step Three: Identify the best immediate and the long-term mobile applications..... 6

 Step Four: Create a mobile security plan..... 6

 Step Five: Develop a mobile policy and communicate to your employees 7

 Step Six: Train your employees on responsible, productive mobility 7

Well planned mobile use changes operations for the better 8

About Sage Construction Anywhere 8



Construction workers are driving inevitable change

In a world of continuous change, the companies that adopt innovation often prosper, while slower, resistant companies often decline. The construction industry is very used to change, and it has already come a long way from a not-so-distant world of manual tools, horsepower, and muscle—to today's sophisticated, precise machinery.

Now, smartphones and tablets have changed the way we all communicate and function, and these new habits are significantly impacting the construction industry.

Construction employees and workers everywhere now expect the type of responsiveness at their job that they experience with their consumer-facing applications. With the expansion of mobile workers everywhere—an estimated 1.3 billion people around the world expected to be mobile by 2015¹—a wide spectrum of business applications is now becoming available, making many options possible.

The majority of construction employees are mobile field workers.² These employees, especially the under-30s generation, are already using personal smartphones and mobile devices at work. A recent study by Engineering News Record revealed 93% of general contractors and 87% of subcontractors use some sort of mobile device at construction sites.³ Other BYOD (“bring your own device”) studies indicate that it's likely your employees are using their personal devices at work, even if your company policy states otherwise.⁴

This change to a world where personal devices are used for work demands management's attention. There are significant security and confidentiality risks if BYOD use is left unmanaged. However, once plans and security are in place, there are strong reasons to let these mobile opportunities happen so that your business can leap forward and benefit from the next level of technological and social innovation.

Know your risks when employees support their own BYOD use

Most companies now permit employees to use their own devices, but only a minority of companies is fully embracing and supporting BYOD use.⁵ The danger is, without clear company policies and practices, employees can unknowingly bring security risk into the work environment. Also, when employees introduce new applications on their own (for example, where files are stored or how one collaborates) employees can collectively bring confusion across projects. However, once security measures and clear BYOD policies are set up, your business will be positioned to adapt both quickly and safely to new mobility opportunities rather than be some hindrance to your employees' good ideas.

1 <http://www.idc.com/getdoc.jsp?containerId=prUS23251912#.UMrgB5PjnC4>

2 www.constructech.com/resources/subscriber_services/Default.aspx

3 <https://enr.construction.com/engineering/subscription/LoginSubscribe.aspx?cid=23761>

4 <http://www.cisco.com/web/about/ac79/docs/BYOD.pdf>

5 http://www.cisco.com/en/US/prod/collateral/routers/ps10537/zk_white_paper_cloudverse.pdf

The BYOD risks

How to minimize BYOD risk

Internet attacks or breaches

Install mobile security software. Ensure corporate data is being kept safe through either Mobile Application or Device Management software.⁶ Set up employee user identity, authentication, and authorizations for mobile access to sensitive company information. Create an internal security plan. (See Step Four)

Use strong mobile passwords. Train employees on how to change passwords regularly and keep passwords safe.

Architect Internet data protection. If company data is accessed from the Internet, use a reputable provider that will provides safeguards. For example, Sage Connector with [Sage Construction Anywhere](#) protects data from direct Internet access.

Select and endorse specific mobile applications. Communicate which applications can be downloaded.

Data leaks and loss of data control

Develop a mobile policy and communicate to your employees. Don't start from scratch—reference template examples found on the Internet. (See Step Five)

Train your employees on responsible, productive mobility. Make sure employees know about general website and email vulnerabilities, mobile malware trends,⁷ and phishing. Reinforce the need for caution when surfing the Internet on their mobile device, just like using a PC. (See Step Six)

Assign one person to monitor trends. Consider electing one technically oriented employee to become your in-house contact for reporting on ongoing security trends and issues.

State your company rights. Publish the company's rights within the company policy guide. For example, list the company rights to erase all email, calendaring, and contact data off the device when an employee is terminated.

Anticipate employee onboarding and offboarding. Include BYOD procedures in your human resource employee checklist.

⁶ http://en.wikipedia.org/wiki/Mobile_application_management

⁷ <https://community.mcafee.com/thread/51061>

The BYOD risks

How to minimize BYOD risk

User application and support issues

Identify supported mobile devices. Consider limiting the number of employee device models to make company support more doable.

Identify the best immediate mobile applications. Limit company applications to those that are easy to implement and have obvious advantages. Over time, introduce any new applications carefully to ensure user acceptance and correct use.
(See Step Three)

Expense surprises

Determine mobile expense policies. Set up policies on what expense is covered and for what type of employee. When there are expenses, create procedures on how to pay employees, whether it's through an allowance program or through reimbursements.

Plan and budget for expenses. If you are paying for an employee's mobile, it may cost \$70 or more per worker per month.⁸

Check your bank statements. If mobile phones are covered by the company, monitor unexpected or suspicious charges.

⁸ http://www.cio.com/article/703511/BYOD_If_You_Think_You_re_Saving_Money_Think_Again

How to implement BYOD policies and mobile applications

Step One: Declare immediate and simple BYOD employee ground rules.

- Take a first step by just declaring some immediate and practical ground rules for all employees. For example, limit where documents can be stored and accessed and communicate the need for mobile password protection.
- Reinforce the mandatory requirement for protecting sensitive documents.
- Tell employees your intention to develop and publish a company BYOD policy guide that includes an employee consent signature.

Step Two: Involve your employees. Get their ideas and input.

- Listening to your employees could uncover the best BYOD innovative ideas for your company. Ask them how they already use their mobile device at work and what else they would like to do. Find out how employees are remotely accessing company information today and discuss together the potential security risks.
- Based on employee discussions, start to create procedures that address how to access corporate data safely. Once it's clear how employees are currently using their devices, determine what measures should be immediately taken to set up appropriate security controls—while staying mindful not to stifle employee innovation.

Step Three: Identify the best immediate and the long-term mobile applications.

- Pinpoint new applications or information that will help employees make wiser, faster decisions. Find the best and easiest applications to implement first.
- Select those vendors you can trust to protect your data for each suitable business application. Common mobile applications include email, customer relationship management, chat, general document storage, note taking, online meetings, and expense reporting. Construction-specific applications may include submitting time sheets, viewing progress reports or business data, accessing the most current drawings or specs or other documents, or collaborating on projects with extended team members.

Step Four: Create a mobile security plan.

- Get outside security advice from industry experts and software providers you trust to determine what security options could protect your company.
- Select a mobile security application that can provide ongoing password protection and remotely wipe company data from a device when an employee is terminated. Ensure corporate data is being kept safe through either Mobile Application or Device Management software.

- Address what levels of access each employee has to what type of company data. (For example, in [Sage Construction Anywhere File Project Files](#) each team member is provided access to only those documents and folders designated important to his or her specific role.)
- Set up employee user identity, authentication, and authorizations for mobile access to sensitive company information.
- Consider setting up data encryption for more sensitive files such as financial reports or customer records.

Step Five: Develop a mobile policy and communicate to your employees.

Don't start from scratch. Keep it readable and easy to digest. You can find different examples on the Internet and modify them for your company. Include the following:

- Clearly explain your expectations for employee productivity and behavior.
- Summarize the prevalence of security risks and threats when using BYOD and the need to keep business information safe.
- Clarify which employees are eligible for using mobile devices.
- State that your business will require security tools and software programs to be downloaded to a device, and these will change over time.
- Define company rights, including company data residing on the device.
- Outline your rights to retrieve or delete information on a mobile device when an employee leaves the organization.
- Explain expense reimbursement policies and procedures.
- Communicate what technical support is provided.
- Obtain employee signature.

When you publish this document, remember the employee. When a company owns and issues its own mobile devices, enforcing policies can be easier. However, in a BYOD environment it's advisable to step lightly if you want to change current behavior.

Step Six: Train your employees on responsible, productive mobility.

The best way to deal with change is to proactively manage it. Let your employees see the good reasons for following new procedures. Any organizational change takes leadership and diligence.

- Train your employees on what mobile uses are supported and what situations are not supported. Educate them on the risks. It's important that you formally present the policies and procedures to your employees to ensure understanding and compliance.
- Encourage employee interaction. Look for ways to encourage ideas. Provide open communications to create the incubator you want for innovation and improvement.
- Train your employees on the new company-endorsed mobile applications.
- Monitor mobile application use and get feedback over time.

Well planned mobile use changes operations for the better

Done right, a well-planned mobile work environment can result in higher employee satisfaction, higher customer satisfaction, increased sales, and increased productivity.⁹ Using mobile devices to access current blueprints, invoices, or project information or to report on activities such as hours, can reduce errors, increase communication, speed up decisions, and reduce travel time between jobsites and the home office.

Making sure employees are safely using their mobile devices on the job is no quick fix, but the effort can be extremely beneficial. Invest first in those solutions that have immediate business advantages but still provide security protection. The time to act on BYOD is now—it's likely your employees already have.

About Sage Construction Anywhere

Sage Construction Anywhere is a cloud-based collaborative solution that connects people, documents, and data securely together in one, easy-to-use, online project hub. It ensures the entire project team can access common, accurate, and timely project information. Sage Construction Anywhere provides Sage 300 Construction and Real Estate (formerly Sage Timberline Office) customers with immediate productivity and operational efficiency through tight integration with Sage back-office financial and operations software—helping construction companies mobilize project information, simplify field-to-office communication, and streamline key back-office processes, like job costing and payroll.

Sage Construction provides project team members with new capabilities to easily store and access project files including documents, drawings, and photos within a centralized, cloud-based location. By using the cloud and mobility technology, users are able to foster collaboration and strengthen communication among the project team to avoid project missteps and delays. Sage Construction Anywhere users are also able to use mobile devices to collect, review, and approve employee time worked on a given project—and then efficiently share accurate, approved labor-related data directly with their Sage 300 Construction and Real Estate job cost and payroll software. This time reporting functionality eases the burden of time collection, review, and approval processes—and provides management with quicker visibility to labor issues in the field so adjustments at the job site can be made sooner.

Visit www.SageConstructionAnywhere.com to learn more.

⁹ http://i.zdnet.com/whitepapers/Profitline_The_Hidden_Risks_of_a_Bring_your_own_Device_BYOD_Mobility_Model_1_19_2011pdf?tag=mantle_skin;content

Sage

15195 NW Greenbrier Pkwy

Beaverton, OR 97006-5701

800-628-6583

www.SageCRE.com
