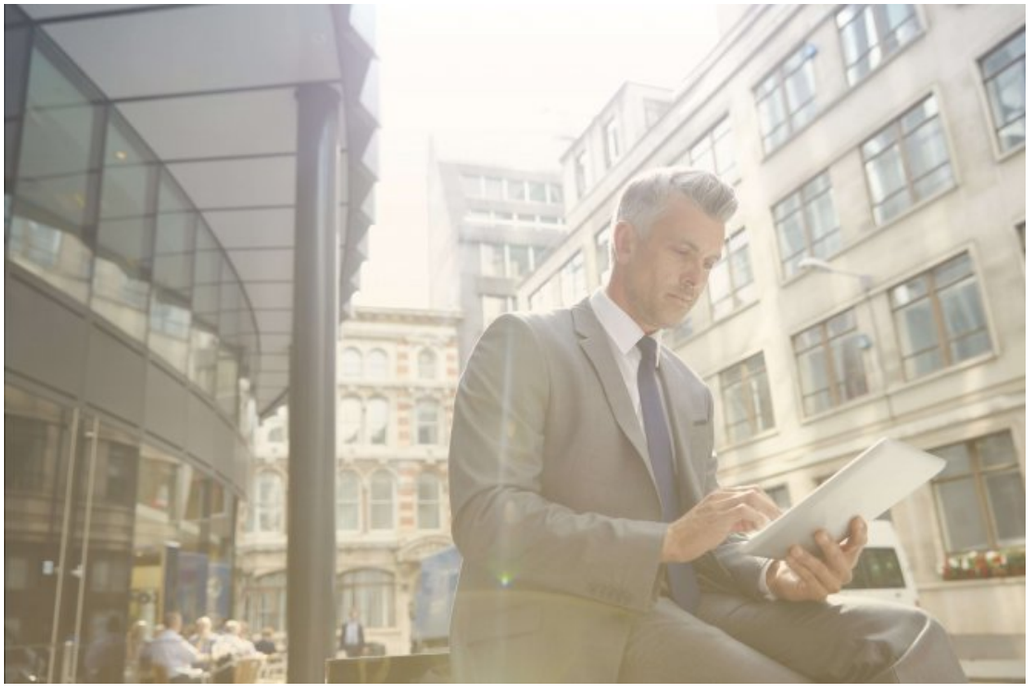
4 Insurance Agency BYOD Questions to Consider

By EVAN WADE - Contributor

For the modern insurance agency, Bring Your Own Device — or BYOD — has gone from an emergent tech trend to foregone conclusion. No longer an unexpected perk, insurance agency BYOD is, at minimum, an option employees expect to have, with employees in most surveys expressing a preference for BYOD-related benefits. As just one example, research curated by TechnologyAdvice says 78 percent of employees prefer to use one device for both work and personal functions.



An insurance agency BYOD policy allows agents to work on the go while minimizing risk.

For an industry that tends to enjoy slower adoption of new technologies, this increased BYOD demand has created several questions regarding policy. For insurance agencies building their own BYOD policies, the following four considerations should remain top of mind:

Insurance Agency BYOD Question 1: Mandatory or Optional?

Do you tell employees they *can* use their own phone for corporate functions, or *require* them to do so? In most instances, this is the number one question surrounding insurance agency BYOD.

Neither path is perfect. An optional program effectively means hedging one's bets, requiring insurance agencies to run a hybrid IT program monitoring both personal and company-issued devices. With mandatory policies, meanwhile, a company may wish to provide

some manner of reimbursement — and may be required to by law in some states.

Both options can also offer substantial benefits. Adopting mandatory policies formalizes the unspoken fact that employees will occasionally use personal devices for work purposes. "Putting it in writing," so to speak, simply allows the company to exert control and minimize risk. Optional programs, meanwhile, give employees a greater degree of choice while giving the organization similar control over both ends of the spectrum. Either way, a choice is coming for these policies — and agencies that haven't yet considered this question should start doing so now.

Question 2: How Will You Maintain Security?

At a high level, BYOD policies are great because they allow insurance companies to access enterprise tools and data on the go. Sales pros courting critical leads or high-tier customer service agents needing insight into troublesome accounts have the liberty of accessing critical data wherever they happen to be. Tools that allow the seamless transition from desk phones to mobile devices — along with those that allow a phone number to "follow" an employee wherever they are, one of several benefits of unified communications — only add to that value.

But there is a cause for concern around portability: When a phone or laptop leaves the office, the risk of unwanted eyes accessing it increases. From the seemingly innocuous friend mindlessly flicking through an employee's phone to a pickpocket grabbing it from their pocket on the subway, it is important to acknowledge that these threats exist. For this reason alone, policies mandating and enforcing strong, private passwords and encryption are a must. Companies should work closely with their IT teams or even outside consultants to ensure they have policies in place that enhance client privacy despite the added risk to portable systems.

Question 3: What Types of Devices?

Another upside to BYOD? All the neat ecosystem features modern OS makers put in their products which can be a real game changer. For example, an employee being able to access the same data from any device they choose is huge — imagine a claims agent being able to snap a picture on her verified BYOD phone, then access it from her laptop at home with no need to send it between the systems through email or similar transmission services.

To keep this benefit from getting out of control, insurance agency BYOD policy should clearly define both the types of devices that are acceptable and the operating systems that are supported. This keeps certain employees from leaning on policy to force the company to accept obscure operating systems and puts a hard limit on the types of devices IT has to support and secure. It can also vastly reduce the complexity of developing mandatory company-specific apps as well as the cost of using software products from third-party vendors. As with any critical policy, the more loopholes a company can stamp out via verbiage, the better.

> *Striking a balance that weighs employee use (they do own the phone and pay for their plan, after all) against enterprise risk is key here. And employee education is, too.*

Question 4: What Should IT Access?

Employees may bristle at the thought, but a risk-averse industry like insurance should consider the level of access IT will have to employee-owned devices. Though the employer may not need total insight into every aspect of the phone's use, access to some areas that would historically be considered "personal" — contents of text messages and call logs as two prime examples here — may be a baseline necessity.

There are also gray areas to consider. While employees can and should be able to access both personal- and business-use websites on their personal devices — such as social media sites or a cloud-based timekeeping or reimbursement platform — but certain malicious sites will unquestionably need blocking to minimize the company's risk of exposure and attack. Most organizations will likely not want to enforce blocking standards as strongly as they would on company-owned devices, but a measure of caution is still both advisable and necessary.

Striking a balance that weighs employee use (they do own the phone and pay for their plan, after all) against enterprise risk is key here. And employee education is, too. Clearly worded policies precluding IT employees from abusing systems to monitor personal use should be implemented, and sanctions against such behavior should be strong. It may take some wiggling to find the right balance, but discovering the mix that keeps the company and its clients safe while keeping employees happy is always worth it.

BYOD has already become the norm in other industries, and insurance appears to be next. The policy raises challenges for the IT team, but each of these challenges can be overcome with some careful consideration. By strategically implementing BYOD in your insurance agency, you'll be able to enjoy the benefits of a mobile workforce while minimizing the risks.