Personal Devices at Work

Resource Type: Articles

Topic: Data Privacy, Tech Risk, Cybersecurity

Employee-owned versus organization-owned… the battle wages on. As employees, many of us prefer to use personal phones and laptops for work because they are convenient, commonsense, and a lot cooler than what the IT department provides. Nonprofits know there is no way to prevent all employees from accessing personal phones at work, so many are creating BYOD (Bring Your Own Device) policies.

On its face, BYOD sounds like a wonderful cost-savings strategy. Employee productivity rises when employees use devices they know and love, and nonprofit employers save time and money as employees cover the cost of purchasing the latest productivity gizmo. The truth is, when you permit or endorse BYOD, you're inviting new and nuanced risks into your nonprofit workplace. These risks run the gamut from privacy violations to data loss and more.

BYOD and Employee Privacy

Smart Savings or Money Pit?

According to Cecil Lynn, electronic discovery counsel at Littler law firm, BYOD does not cut costs. Lynn estimates a typical mobile BYOD environment costs 33% more than when a company owns the devices. Lynn says BYOD programs cost more than organizational ownership of IT devices because companies lose bulk purchasing power, they provide greater tech support for personal devices, and security risks are hard to budget and often wind up costing more than imagined.

It's important to recognize that employees may need to forfeit privacy rights in exchange for the freedom to use personal devices at work. By accessing work information on a personal device, an employee puts a nonprofit's assets and reputation at risk. Employees might lose their phones, forget to encrypt work emails, or open unsecured Wi-Fi hotspots accessible by unknown external users. Even after an employee is terminated, risk remains. A former employee could bring the personal device to a new job and leak or inadvertently share sensitive information with their new employer.

To manage BYOD risks, nonprofit leaders should implement defense strategies; unsurprisingly, many defenses reduce employee privacy. For example, nonprofit IT departments may install remote access apps on personal devices, so IT administrators can access information when necessary. If an employee misplaces a phone used for work, the IT administrator can access the phone remotely and delete any sensitive organizational data.

Unfortunately, when such a remote access app is installed, personal documents like photos and videos may be accessed and deleted as well. IT staff may also be required to safeguard information by blocking network access, apps, and websites on personal devices. Nonprofit employees may view these acts as breaches of privacy or personal rights.

BYOD Risks to Nonprofit Employers

Aside from data breaches or the risk of a terminated employee sharing trade secrets with new employers, top BYOD concerns arise from the employment relationship.

- Workplace safety risks: While driving, employees may talk on personal devices that are used for personal *and* work reasons.
- Labor law risks: IT safeguards protecting a nonprofit's reputation and assets may be considered unlawful surveillance of employees.
- Wage and hour risks: Personal work devices used off-the-clock for business purposes may put the nonprofit employer at risk of liability for overtime time pay.
- International risks: When employees travel abroad, border guards may access sensitive data while searching devices.

BYOD use also exposes nonprofit employers to the potential for leaked contracts, leaked client/ partner information, and the risk of employees uploading materials to servers owned by other companies (e.g., through the use of cloud apps like Dropbox or Google Drive). If your nonprofit aspires to best-in-class risk management as a framework for BYOD use, consider putting the following safeguards in place:

1. Create a clear policy on BYOD rights and information security rules.
2. Train employees to protect work information accessed on personal devices.
3. Require employees to sign an agreement acknowledging their role in protecting confidential or personal information stored on or accessed by personal devices.
4. Require employees to sign an agreement acknowledging the actions and steps an in-house or outsourced IT team may take to protect information stored on or accessed by personal devices.
5. Establish a protocol for wiping work-related information from lost employee devices or when separation from employment occurs.
6. Ban employees from moving funds into or out of nonprofit bank accounts using personal devices.
7. Prohibit non-exempt employees from accessing work email or making work-related calls outside of work hours, or establish clear guidelines with appropriate accountability measures permitting work outside approved schedules.
8. Consider establishing a partnership with a mobile service provider in which the provider polices information accessed on personal devices in real-time under a security agreement.
9. Offer resources like AT&T Toggle to employees, allowing them to distinguish 'work mode' from 'personal mode' on a smartphone.

No matter how many BYOD policies you create, risk remains. An IT department charged with securing nonprofit data can offer only partial protection for data stored on devices the nonprofit doesn't own. But, even if you stick to organization-owned devices, data breaches may occur. Weigh the upsides and downsides of BYOD versus organization-owned; decide whether your nonprofit is in position to take advantage of the benefits while managing the downside risks.

Additional BYOD Questions

As you design a BYOD policy or adapt a policy to reflect your existing practice, take time to address the following issues:

- Are employees responsible for equipping personal devices with software needed for work tasks?
- Who maintains the personal device hardware and software — the employee or the IT department?
- How will personal devices be linked to the nonprofit's network while minimizing the spread of malicious software (malware) and viruses?
- Will employees consent to IT staff having access to personal devices?