Can Geofencing Help Make Mobile Devices More Secure?

By Christine
Kern

Security is at the forefront of concerns across enterprises these days, and everyone is searching for new ways to protect their data from misappropriation and misuse. Geofencing technology could add an additional layer of security to ensure the protection of sensitive information in a variety of ways.

According to a Cisco report, 70 percent of IT professionals stated that they believe the use of unauthorized programs resulted in as many half of their companies' data loss incidents, and 39 percent reported that they have dealt with an employee accessing unauthorized parts of the company's network.

Geofencing allows IT administrators to set geographic boundaries indicating secure areas and gives mobile device management (MDM) clients granular control over their employee's devices, while respecting their privacy when outside of the office, according to *Skyhook*. Your government, enterprise, and educational clients, especially, could benefit greatly from this ability.

Geofencing can also ensure document security. One significant application is securing patient medical records and information, whose security is governed by The Health Insurance Portability and Accountability Act of 1996 (HIPAA). HIPAA addresses the technical safeguards that organizations must put in place to secure individuals' "electronic protected health information" (e-PHI).

Geolocation technology can help secure medical records and data by ensuring the proper access to this information. For instance, a hospital may want to grant its doctors access to patient records only inside hospital walls and in the security of their homes. Through MDM, your hospital clients can geofence not only their property but any location they deem secure.

Romania-based CoSoSys has also added geofencing to its mobile device management software, tracking locatior via GPS, Wi-Fi and Bluetooth beacons. The system works because it uses local beacons, as well as the GPS location to pinpoint exactly where the device is located, according to *CSOOnline*.

Geofencing can be used to restrict access on visitor devices, track employee devices, or restrict access, or used with tablets, "to 'brick' a device, limiting it to only certain applications off site or after work hours.

However, despite the possibilities that geofencing offers there are still issues related to privacy and security — the GPS lock can be spoofed —that must be overcome before it could be used mainstream.

CoSoSys founder and CEO Roman Foeck asserts that these are challenges that can all be addressed, and stressed that using GPS in combination with other location mechanisms is really the key. "If you rely on a second factor — like proximity to some other devices, such as secure beacons that act as tokens — that cannot be spoofed," he says.