Pokemon Go and BYOD

Pokemon Go has caught on around the US and shows no signs of slowing down. People are downloading the app in record numbers, and everyone from children to adults are capturing Pokemon everywhere they go. This raises serious issues for employers who allow employees to use their own devices in the workplace.

Michael Whitener, partner with VLP Law Group, was recently quoted in the *Inside Counsel* article, "Pokemon Go Exposes the Risks of BYOD Policies," discussing the potential data security concerns this app raises for employers.

According to Whitener, "Because Pokemon GO has been so enormously popular – reportedly the most downloaded mobile game ever, with more than 25 million users playing each day – the security concerns of the game have received wide publicity."

He goes on to say, "The Pokemon GO security issues have been a wake-up call to businesses that permit use of personal mobile devices for business purposes, but have not put in place either a BYOD policy that employees must comply with or security measures for protecting corporate and personal information from unauthorized access that apps such as Pokemon GO may enable."

Employees want the freedom to use their mobile devices for both work and personal use, and that mobility and ability to work "on the go" is also important to employers. Therefore, there must be a balance between leveraging the advantages of BYOD and protecting data, and that means implementing a realistic BYOD policy.

Whitener says, "Employers will need to adapt their security protocols and BYOD policies to employee demands rather than the reverse. The balancing act between employee flexibility and corporate security will continue, but the trends toward greater mobility and the blending of personal and professional lives are unstoppable."

Click here to read the full *Inside Counsel* article.

Michael Whitener is a VLP Partner. His legal practice focuses on two areas: (1) technology transactions and (2) data privacy and cybersecurity. Michael provides practical advice on the collection, use, sharing and protection of data in compliance with an ever-changing network of privacy laws. He conducts privacy audits and risk assessments, drafts privacy/security policies and data transfer agreements, advises on compliance with U.S. and foreign data privacy laws and regulations, and assists companies in preventing and responding to data security incidents.