From the Kansas City Business Journal:
http://www.bizjournals.com/kansascity/news/2016/09/09/tech-orchard-panel-how-employers-can-address.html

Tech Orchard panel: How employers can address mobile security issues

SUBSCRIBER CONTENT:
Sep 9, 2016, 2:28pm CDT

LESLIE COLLINS | KCBJ

Overland Park-based Tech Orchard hosted a mobility panel discussion Thursday evening, which featured Keith Shaw (from left) of H&R Block Inc.; Cora Belfiore of Winston & Strawn LLP; Randy Crenshaw of Tech Orchard; and James Robertson of Core BT Solutions.

Mobile security and mobility are hot topics in the corporate world.

Years ago, the focus was ensuring the back-end network was secure, but now the greater focus is on apps and protecting mobile devices, said Randy Crenshaw, vice president of mobile technology at Overland Park-based Tech Orchard.

Crenshaw shared his insight as part of Tech Orchard's mobility panel discussion Thursday evening at the Boulevard Brewing Co. event space. Other experts on the panel were Keith Shaw, manager of security engineering and operations for H&R Block Inc.; Cora Belfiore, director of IT operations at Winston & Strawn LLP; and James Robertson, owner of Core BT Solutions.

In the U.S., 198 million households now have mobile devices, Shaw said. And those devices bleed into work and play. Employees use both corporate-issued and BYODs (Bring Your Own Device) to perform work duties, whether that's using an app or particular software or sending email. It's crucial for employers to ensure that those devices and apps are secure, and an avenue for doing that is installing enterprise mobility management (EMM) software and malware threat protection (MTP). EMM protects the mobile device from security threats as well as the data that rests on the mobile device and the data that's being sent to and from the device. MTP also protects the device, in addition to the network and applications that run on the device.

"In your enterprises, especially, with BYOD, people have a real concern for privacy, and they may not all be excited about having an EMM product on their device," Crenshaw said.

Winston & Strawn witnessed that in November. The law firm had delayed implementing EMM software on employees' devices but finally took the leap last year.

"I did have people that were really questioning why we have to do it now, when we had already let them on the network. Why did we have to secure the device now?" Belfiore said.

There were several keys to getting the firm's lawyers on board, she said. The firm gave employees 30 days to install the software and hosted beer and pizza parties, where employees could enroll their devices. She also emphasized the client perspective – that it was about protecting their data, too. Once employees understood the benefits to clients, they really got on board.

Robertson also highlighted the importance of EMM.

"We really view security and EMM as a checkbox. It's something you have to do. It's at the top of the list," Robertson said.

Employers also must develop effective security awareness training, Shaw said. One aspect that's often missed in that communication, however, is mobile devices, he said. One of the past companies Shaw worked for discovered an employee who was surfing porn at home on a corporate-issued mobile device. The employer tried to terminate the employee, but the employee said: "Tell me where it says I can't do it? Where did you publish this?"

It's crucial to have those expectations and policies in writing and effectively communicated to employees, he said. Crenshaw added that it's also a good idea to have employees sign a mobile device usage policy when they receive their device.

Leslie Collins
Web Producer
Kansas City Business Journal