- We want to consider how do we protect our employees and our businesses as they use mobile devices throughout their day-to-day jobs.

In 2014, it's estimated there's over 7.4 billion mobile devices on the planet. That now exceeds the number of people on the planet. Everyone wants access to everything from everywhere, and simply put, we can't be everywhere as a security team all the time. So, we're constantly having to revise and devise new measures to protect those mobile applications, those mobile users, as the connect back into the corporate infrastructure.

It's no longer today the traditional mindset of putting everything behind a castle wall, behind and moat, and saying, "You can only come through one entry point."

Now, there are millions, literally billions of entry points to any given network and the security teams, the technology teams, have to understand how those occur, who has the access, and then come up with the right controls to protect against any threats.

The desire for employees to bring their own device has really complicated the IT environment for the technology team. It's not just the security aspects of it, but thinking about the interconnectivity that you have to allow those devices, the very ability in number and type of devices that are gonna be connecting. And mobile app developers, they develop very quickly, very rapidly, and we'll talk about in the next essential practice on application security why security needs to be part of the development life cycle. So you have to think about it really end to end, from the user of the mobile device and how you have access control there, how you protect the mobile device and the data on it and what you consider
authorized use for that device, and then the types of applications and data you permit that device to access. You may not want to permit it to access some of your most sensitive or confidential corporate information. Every business has to decide what's acceptable and allowable for them, and how much risk they wanna pose to their environment and their data by allowing their employees to connect to it with their mobile devices. In 2014, IBM undertook a study of mobile application security. We looked, actually, at dating applications and the types of vulnerabilities you would find in them, and we found that in about 60% of the Android applications, there were vulnerabilities that would allow an attacker to access personal or other confidential information on that mobile device. In about 50% of the organizations we surveyed, those same mobile devices are accessing corporate infrastructure. So, what's really happening is the employee or the person is putting not only their own personal data at risk, they're also exposing, potentially, corporate confidential or sensitive information when they use their personal mobile device for business use. And many companies are struggling with the complexity of how they secure those devices, those personal devices, within corporate environments. There are many different technology solutions available, but ultimately, if we think back to risk-aware culture in essential practice number one, we have to educate them on the risks of using that and the shared risk that both the employee faces by accessing the corporate information with their personal device, and that the company faces by allowing the use of personal devices in their environment.