SESSION TITLE	Six Things Wireless Security Professionals Need to Know About Wireless
SESSION QUICK ABSTRACT	Top six things every security professional need to understand about wireless networks to be effective in handling the growth of mobile devices, BYOD deployments and IoT implementations.
SESSION SHORT ABSTRACT	The growth of mobile devices, BYOD deployments and IoT implementations make it critical that security experts understand how wireless works. This session is a unique opportunity to hear from wireless implementation expert Dr. Avril Salter as she explains the top six things you need to understand about wireless networks that will make you more effective as a security professional.
SESSION DETAIL	Dr. Avril Salter, renowned wireless expert, continues to be amazed by how many security professionals she meets that have only a rudimentary understanding of how wireless networks work. The growth of mobile devices, BYOD deployments and IoT implementations, make it even more critical that security experts understand how wireless works. If you answer “no” to any the following questions then you need to attend this session. 1. Is it possible for a security professional to protect their organization’s wireless networks if they are not aware of how wireless networks work? 2. Can you make an informed security assessment for your business without knowing how signals propagate over-the-air, or how antennas impact signal reception? 3. Are you comfortable performing penetration tests on your organization’s wireless network without being familiar with wireless network topologies and architectural alternatives? 4. Can you investigate and react to attacks without an in-depth understanding of wireless network configuration settings?

	This session is a unique opportunity to hear from wireless implementation expert Dr. Avril Salter, as she explains the top 6 things you need to understand about wireless networks that will make you more effective as a security analyst, wireless administrator, or network security specialist. Topics covered include: ● Deploying antennas to limit or extend Wi-Fi coverage. ● Using wireless traffic analyzers to check over-the-air security settings. ● Assessing wireless network attacks with spectrum analyzers and packet analyzers. ● Configuring access points and clients to optimize throughput and coverage while reducing security risks. ● Avoiding configuration changes that lead to disaster. At the end of this session attendees will be able to: ● Describe how antennas (including MIMO antennas) are used to limited coverage and extend the range at which one can eavesdrop on wireless traffic. ● Interpret packet captures to determine security configuration settings. ● Understand how spectrum analyzers and packet analyzers can be used in combination to analyze wireless attacks. ● Evaluate the implication of key wireless configuration settings and its effect on the security and usability of the wireless network. Dr. Salter will share with the audience real life deployment scenarios based on her 25 years of experience in working in the wireless communications industry.