

Brief Summary of the ATIC Cyber Security and InfraGard Public Information Meeting

An Arizona Telecommunications and Information Council (ATIC) (<http://www.arizonatele.com/atic/>) Public Information Meeting was held on Thursday, November 19, 2009. This was the final ATIC Public Meeting for 2009 and it focused on cyber security. It was held in conjunction with InfraGard Phoenix (<http://www.phoenixinfragard.net/>) at the law firm of Lewis & Roca LLP (<http://www.lrlaw.com/>) in downtown Phoenix (40 N. Central Ave., Renaissance Two Building).

Ron Schott, Chair of ATIC, opened the meeting with a welcome to nearly 70 people in the audience and about a dozen remote (via teleconference) attendees. Ron then introduced the moderator for the session, **Jerry Crow**, chair of the ATIC Cyber Security Committee.

Jerry, who is also the InfraGard Phoenix Program Director, noted that this marks the Third Annual Fall Joint Meeting between ATIC and InfraGard. He then introduced the first presenter **Jim Ryan**, Chief Information Security Officer (CISO) in the Statewide Information Security & Privacy Office (SISPO) of the Government Information Technology Agency (GITA) for the State of Arizona (<http://www.azgita.gov/sispo>).

Jim noted that the objective of cyber security is to protect information and critical infrastructure from internal and external harm, while allowing the owning agency to function productively. Although considerable protection policies are in place, such as statewide policies and standards, third-party compliance audits and 24/7 monitoring of the statewide area network (WAN), more needs to be done. From a business perspective, among other things, we need to focus more on risk management regarding protection of data and infrastructure. From the point of view of technology, there is a need to focus on the automation of vulnerability scanning and compliance reporting. Jim summed up the overall objective of cyber security as consisting of privacy being the goal, security is the journey, technology can help but people are the key.

Jerry then introduced the next speaker **Paul Schaaf**, Special Agent for the Phoenix Office of the Federal Bureau of Investigation (FBI) (<http://www.fbi.gov/>).

Paul focused on cyber threats that are becoming increasingly common today. He briefly reviewed the Zeus Trojan for Automated Clearing House (ACH) fraud, the well-known Conficker worm, SQL injection techniques, phishing and its more targeted relative spear phishing and the ever-present internal threats. Paul also spent some time summarizing the recently released supplement to Verizon's "2009 Data Breach Investigations Report" (see <http://securityblog.verizonbusiness.com>). That report aims to provide both technical personnel and managers with a one-stop compendium of pertinent

details on the widespread threats in existence. Hopefully this information can be used to prepare for, detect and, ideally, prevent these types of attacks. Paul identified some other useful organizations that people should know about to protect themselves from cyber threats. This list includes the Internet Crime Complaint Center (IC3) (see <http://www.ic3.gov>), which is a partnership between the FBI, the National White Collar Crime Center (NW3C) (<http://www.nw3c.org/>), and the Bureau of Justice Assistance (BJA) (<http://www.ojp.usdoj.gov/BJA/>).

Following Paul's presentation, Jerry introduced **Brett Scott**, the Chief Technology Officer for LiveSquare Security (<http://www.LiveSquare.com>).

Brett gave a sobering account of the reality and potential dangers of cyber warfare. More than 120 countries have or are developing cyber warfare capability. The arenas of activity include the international scene, where the players come from industry, the military and intelligence organizations; criminal ventures, consisting of lone operators as well as registered companies; and the political environment, which specializes in flooding web sites and communication systems, spreading disinformation and other types of "hactivism." Today the main players in cyber warfare are China, Russia and the United States. Brett reviewed some of the challenges the United States faces to improve its footings in this arena. He called for a move to a merit based security and prevention system where everyone can play, increased cooperation in the security industry, the creation of coalitions of collaborators and what he termed as a "caustic cauldron" of community based entities for testing security techniques and procedures. Two groups that are worth considering joining are the CYBER SECURITY Forum Initiative (CSFI) on Linked-In (see <http://www.linkedin.com/groups?gid=1836487>) and the Open Web Application Security Project (OWASP) at <http://www.owasp.org/>.