Cybersecurity needs and opportunities in the MICS region.

ABSTRACT

A stable, safe, and resilient cyberspace is vital to our economic vitality, national security, and personal lives. We depend on the networks for a variety of services that impact our ability to communicate and travel, power our homes, run our economy, and provide government services. Over the last decade cyber intrusions and attacks have increased dramatically making cyberspace a dangerous place, if one is not careful. Sensitive personal and business information are all at risk in this in interconnected world. It is claimed that theft, fraud, and abuse is costing American companies upwards of $250 billion a year.

In an article by Charles McLellan, “Cybersecurity in 2015: What to expect,” he examined forward-looking articles from 17 organizations and assigned the resulting 130 predictions to a number of emergent categories. At the top of the list are “New attack vectors & platforms” and “Evolution of existing cybersecurity solutions”. The “New attack vectors & platforms” is essentially, "new bugs in old, widely-used code". For example, FireEye noted that "Apple's increasing enterprise footprint means malware writers will adjust their toolset" and that record sales figures from Apple will only increase the hacker’s appetite to attack Apple products. The second category, “Evolution of existing cybersecurity solutions,” included ImmuniWeb's contention that "Automated security tools and solutions will no longer be efficient" if used independently or without human intervention.

The intent of this panel is to discover what cybersecurity concerns our regional employers face, what they would like to see from the institutions of higher learning (with regards to cybersecurity education), and what options do the institutions of higher learning have for trying to meet these demands.

This panel will include representatives from the region’s employers of computer science graduates as well as the region’s only member of the National Security Agency’s (NSA) National Centers of Academic Excellence (CAE) in Cyber Operations Program. The list of panelists includes representatives from Dakota State University; DigiKey; Fast Enterprises; and Rockwell-Collins. The panel will be moderated by Ronald Marsh, Ph.D. University of North Dakota.

Kevin Streff, Ph.D., Dakota State University: Dr. Streff performs information assurance management research in the financial services sector, with a particular focus on understanding the security issues of small and medium-sized financial institutions. On the research side, Dr. Streff is founder and director of the National Center for the Protection of the Financial Infrastructure, which is a consortium of universities working together to fortify the resiliency of the electronic critical infrastructure of the financial sector. On the teaching side, Dr. Streff led Dakota State University to be named a National Center of Excellence in Information Assurance Education through the National Security Agency and the Department of Homeland Security. He teaches managerial elements of information assurance, including risk management, security policy, information security management systems, disaster recovery, business continuity planning, and incident response planning. Dr. Streff has 50+ publications in peer-reviewed journals and is PI of over $5 million in grants over the past five years, including awards from DHS, NSF, and NASA. Dr. Streff is also founder and managing partner of an information security consulting and auditing firm which now employs 70 security professionals and works in 12% of the banks in the United States. He also has extensive knowledge of the financial services industry, including commercializing research to meet market needs. He is also founder and past-President of InfraGard South Dakota, an outreach program to promote the protection of critical infrastructure in SD, ND and MN. Prior to coming on faculty at Dakota State, Dr. Streff worked in the financial services industry for 15 years.

Isaiah P. Grothe, Network Engineer, Digi-Key Corporation: Confidentiality, integrity, and availability: the goals of cybersecurity. There are many challenges to achieving these goals, and the threats and countermeasures are continually changing. Most corporations today, including Digi-Key, would find it nearly impossible to remain viable in business without the aid of technology. Compromising any of our three goals of security quickly causes the entire model to crumble. And yet, of the measures that we need to take for security, most are themselves constraining. Security is often inversely proportional to convenience, but it is also essential, so it is a juggling act.

Some particular areas of challenges for Digi-Key:

- Digi-Key does a significant percentage of its business with credit cards, and thus is subject to PCI-DSS regulations. Compliance is not an end of security and does not even guarantee robust security, but is rather a starting point and an incentive.

- Digi-Key has a large web presence and conducts over 80% of its business directly from its website. This large presence equates to significant exposure to web-based threats. Digi-Key is also aggressively expanding its presence around the world in locations such as China and Europe, and that also increases its visibility and allure for threats.

- Digi-Key develops most of their internal systems, such as the web site, ordering, inventory, and material handling systems in-house. That being the case, there is continuous development and changes for security to stay ahead of and involved in order to guarantee a secure architecture.

- Digi-Key has over 3,300 full and part-time employees and also many contractors. There are many differing roles and with differing needs and the challenge lies in managing them according to the principles of least privilege and need to-know, all while not being overly impeding. User awareness is also something that needs to be continually addressed, as the human factor can often be one of the weakest aspects of security.

Evan Sylvester, Information Security Officer, FAST Enterprises, LLC.: A Certified Information Systems Security Professional (CISSP) with 10 years of academic and professional experience. Evan has received an MBA from Texas State University and a BBA in Management Information Systems from the University of Texas at Austin. Evan regularly attends multiple security conferences a year including DEFCON and Security B-Sides. Evan maintains several industry certifications related to networking/security and is currently working towards others.

Donald Kearney, Senior Engineering Manager of the Airborne Information Systems Platform Security group, Rockwell-Collins: Mr. Kearney is one of the security experts responsible for leading a team of engineers whose charter is to protect the information flowing within the various systems on board an aircraft and between our systems and our avionics customers on the ground.