Education in cyberspace security

By Elijah Morlett
Assistant Managing Editor

On Sept. 15, Cameron's Department of Computing and Technology hosted a seminar about cyber security that focused on balancing technology, educating users and making policies to provide maximum information technology.

The department brought in guest speaker Benjamin Carlson, a Computer Network Defense Team member for the State of Oklahoma Military Department, to explain some of the history and ongoing trends with cyber security.

"Computer viruses and bugs have been written about and discussed for over 30 years," Carlson said. "Most users do not understand how unsafe and insecure the Internet is."

In addition to serving in the Oklahoma Military Department as a soldier, Carlson also works for CGI Federal as a radar software engineer and has worked as a computer scientist for the United States Navy at the China Lake Naval Weapons Research Lab.

Also discussed was the onset of new technology in the work environment. While the technology is present to make jobs easier, Carlson says that venturing quickly into the new systems can become risky.

"People rush into new technology before it's ready," Carlson said. "For example, cloud computing is the newest thing right now. While companies say it is safe, new issues can arise soon."

According to Carlson, a balance in policy and user-education is necessary in organizations. Over-emphasis on policy may lead users to abuse the system more, while education may prove to be more preventative.

"There's more focus on new technology and less on user education and user compliance," he said.

User education emphasizes the practice of using the Internet cautiously and safely, knowing what to avoid and what may be harmful.

"User education needs to be applied at home as well as work," he said. "Employees may not know that they could be bringing computer bugs from their home."

According to the information at the seminar, policies must match education. Carlson said that policies should not cause too many issues with employees and policies should be discussed with IT staff and managers.

"Unrealistic, impotent or conflicting policies should not be implemented," he said. "This will generally cause users to ignore all policies."

While organizations should plan for implementing cyber security protocols, Carlson said that there is no completely protective security.

"Organizations need to plan as though security will be breached," Carlson said. "There will never be perfect security. Companies must have a solid plan for dealing with incidents, for they will occur."

Even though the seminar primarily focused on the IT aspects of organizations, Carlson said that these standards should reflect in the daily lives of all Internet users, including students.

"Students need to be careful and thoughtful about running into things online," Carlson said. "Identity theft is still a major issue, so don't treat the Internet as a playground. You can easily lose a lot of money or damage your reputation."