"Federation Corner" column
The Montgomery Sentinel - May 22, 2014

How vulnerable are county computers?
by Jim Humphrey
member, MCCF Executive Committee

An interesting exchange took place in the Montgomery County Council hearing room on May 6 between Council members and officials addressing the FY15 Operating Budget request for the county Department of Technology Services.

As reported by another area newspaper this week, the exchange seemed to focus on the fact that old computer software programs, which are no longer being supported or updated by Microsoft, have led to Council members Microsoft Outlook scheduling calendars not automatically synchronizing with their mobile devices.

“This is not a matter of personal convenience. It’s a matter of Montgomery County business,” said Council President Craig Rice (D-District 2).

“I am totally dependent on my calendar to tell me where I have to be and when. Without it, I am totally lost,” said Council member Roger Berliner (D-District 1). Berliner added. “I am now having my staff print out and fax me my calendar.”

I am sure that this screw up with the scheduling app on their mobile devices is irksome to our elected officials, especially since they are in the thick of campaign season with seven of the nine members of Council seeking reelection to their seats and an eighth member running for the County Executive spot. (Remember that the ninth member, Council member Cherri Branson who represents District 5, promised not to run for reelection when she was appointed to replace Valerie Ervin, who quit before the end of her term.)

But, boys and girls, let's get our priorities straight. The real problem at issue here is the extent to which the use of outdated hardware and software has made the county's computer systems vulnerable to attack by hackers.

Although nothing approaching a level of sufficient resources has been allocated for the job, I guess it is somewhat reassuring that the issue of cybersecurity is at least on the radar of some of our county officials.

The three members of the Council Committee on Government Operations and Fiscal Policy (Chair Nancy Navarro, Cherri Branson, and Hans Riemer who was appointed last year as Lead Member for Digital Government) wrote in a March 14, 2014 memo to the county Department of Technology Services Chief Information Officer Sonny Segal:

"We are all well aware that cyber attacks pose a very serious threat. In addition to highly publicized attacks like the Target breach, the Identify Theft Resource Center reports that there have already been 130 major data breaches in 2014 which exposed more than 2.8 million records. That number includes breaches of state government systems in Iowa, Oregon, California, Connecticut, North Carolina, and South Carolina and systems operated by the City of Detroit and the Memphis Police Department. It is not a question of if Montgomery County government will be targeted, but when."

The purpose of the March 14 committee memo was to stand the Department of Technology Services on notice that when their FY15 Operating Budget came up for review this month, the Council would be relying on a document entitled the Cybersecurity Strategic Plan to assess whether the County Executive's budget request was sufficient to address the highest priorities. Unfortunately, only a draft of the Cybersecurity Strategic Plan has to date been transmitted to Council (in February of this year), yet the county government budget is being adopted by Council today, May 22.

In his May 2, 2014 memo to the Council, Internet Technology Adviser Dr. Costas Toregas stated that in early April, "The (Government Operations) Committee requested that the Executive release the Cyber Security Strategic Plan soon, and make supplemental appropriation requests appropriate to the task at hand and commensurate with the high degree of risk that is evident, given the reliance of the County's entire business processes on technology." However, Toregas goes on to say, no such funding is evident in the Executive's recommended budget, with the exception of three new programs adding $280,000 for "training, policy, and risk assessment."

One item that was targeted for $97,000 in funding in the FY15 budget, however, is the Interagency Web Search Project, which is planned to "strengthen citizen access to information...that current search solutions do not easily reveal." In layman's terms, they want to beef up the Google Site Search capability to enable users of the county government website to "quickly and accurately search by keyword or phrase to discover relevant content that is distributed among County agency websites."

I am not sure how important a better search capability on the county website will be if the county is unable to protect sensitive personal information from being grabbed by hackers--like homeowners' bank account information used to pay property tax bills, or credit card information used to buy time on our fancy, new parking meters.

I might feel like information which the county collects on its residents and businesses was a tiny bit safer if the word "security" even appeared in the mission statement for our Department of Technology Services. But it reads, in full: "The mission of the Department of Technology Services is to use information technology to enable our employees to provide quality services to our citizens and businesses, deliver information and services to citizens at work, at home, and in the community, and increase the productivity of government and citizens."

I guess we should be content that the experts in the field of internet security with our local government are furiously working toward a solution that will quickly provide a state-of-the-art level of protection for the data management systems of one of the richest counties in the United States.

After all, as Department of Technology Services Chief Information Officer Sonny Segal wrote to Council in a memo in early May, "I am requesting to brief the GO Committee on the outcome of the Risk Assessment and penetration testing as well as the progress made during initial phase of implementing the Office 365, and the accelerated Cybersecurity Program in September 2014." Zippedy-do-dah.

The views expressed in this column do not necessarily reflect formal positions adopted by the Federation. To submit an 800-1000 word column for consideration, send as an email attachment to montgomerycivic@yahoo.com