Rock Hill Herald Online

Next Story >

**Don't be fooled by York County alcohol referendum**

# S.C. data breach shows need for one computer system

Published: November 10, 2012

By Richard Eckstrom — Special to The Herald

If it can happen to computer systems maintained by the U.S. Department of Defense, it can happen to anyone's computer system.

That's not an excuse. But it's a disturbing fact in today's increasingly networked "cyber world," as organizations constantly combat hackers determined to breach any computer safeguard to steal sensitive information.

I'm not minimizing the seriousness of the recently announced S.C. Department of Revenue data breach, in which foreign hackers apparently got their hands on tax records of 3.8 million South Carolinians and more than 650,000 businesses. However, the reality is that virtually no system is immune to this kind of threat.

For example, hackers have broken into Pentagon computer systems on at least three occasions since 2008, according to published reports. In one of the incidents, files on the military's next- generation F-35 Joint Strike Fighter were copied.

Some security experts might be surprised that personal identity theft doesn't happen more often. Think about all of the times you've been asked for your Social Security number: when applying for loans; applying for jobs; discussing accounts with utilities; buying health insurance coverage. It's even a standard request when donating blood.

For that matter, not too many years ago health insurance cards and individual pay stubs had Social Security numbers routinely included on them. It was common practice for people to have their pre-printed Social Security number included on their personal checks, and if that information wasn't pre-printed on your check, vendors would ask you to write it manually.

Stop and think about how often everyone's Social Security number has been vulnerable to compromise at one time or another – if someone of ill intent wanted to use it. Having said that, we as a state and as individual South Carolinians should do everything we can to protect ourselves against cybercrimes like identity theft.

Thoughtful minds are asking what else state government should be doing to protect data. One answer is pretty clear, yet achieving it will be complicated if territorial concerns fight against what's in the more pressing interests of taxpayers. We need to consolidate the stand-alone computer systems of all state entities so that our expertise, energies, and resources are pooled rather than fragmented.

The recent implementation of the S.C. Enterprise Information System (SCEIS) was a significant step toward this goal. It brought the core accounting, payroll, procurement and human resource operations of most state agencies into one system.

But state-supported colleges and universities, and various programs at some state agencies, are not part of any unified system. It makes little sense for any state entity to proceed on its own rather than using all of the available resources of state government to protect against computer-savvy hackers.

The S.C. Division of State Information Technology (DSIT) already manages and provides information technology services for a large swath of state government. Those services even include monitoring and testing for data breaches – at no charge.

The Department of Revenue was not among the state agencies covered by DSIT prior to this data breach, although it is now. This is not to say that the breach absolutely would have been prevented if the Department of Revenue had been part of the state's consolidated system. That can't be guaranteed. Being part of the state's system certainly wouldn't have hurt, though.

Centralizing our computer systems wouldn't just bolster security. It also would allow the state to weigh and prioritize its options for how to capture information needed for making better decisions and holding agencies more accountable for performance.

Unfortunately, my office sees the shortcomings of the state's fragmented, decentralized computing and accounting systems every year in gathering financial data to produce the state's monthly and yearly financial reports. This fragmented structure is often inefficient.

To put it bluntly, some state-supported colleges and other agencies operate like independent nations rather than as partners on a team, resulting in duplicative systems. Duplicative systems penalize taxpayers with inefficiency and with avoidable costs.

In taking stock of this recent hacking case, it's important that we don't politicize it or use it to push other agendas. Instead, let's use it as a learning experience to help state government better serve its ultimate constituents – the taxpayers.

It would be a double loss, indeed, if government returned to business as usual by accepting the unnecessary costs and risks of allowing many state entities to operate their own computer systems rather than safely consolidating them under the watchful eye of dedicated experts.

Richard Eckstrom is S.C. Comptroller General.

Back to Top
< Previous Story

**Gun-show 'loophole' is complicated issue**

Next Story >

**Don't be fooled by York County alcohol referendum**

Email Newsletters >
Manage newsletter subscriptions
Tablets >
Apps and services for tablet devices
Mobile >
Apps and services for your mobile phone
Social Media >
Get updates via Facebook and Twitter
e-Edition >
Your daily paper delivered to your computer