

SILICON VALLEY BUSINESS JOURNAL

August 15, 2014

Governments and data security

Earlier this month, a computer security firm broke the harrowing news that hackers had stolen 1.2 billion login credentials from more than 420,000 websites. This is certainly the largest but only the latest breach of personal information to make headlines. In December, thieves pilfered 40 million credit card numbers from retailer Target.

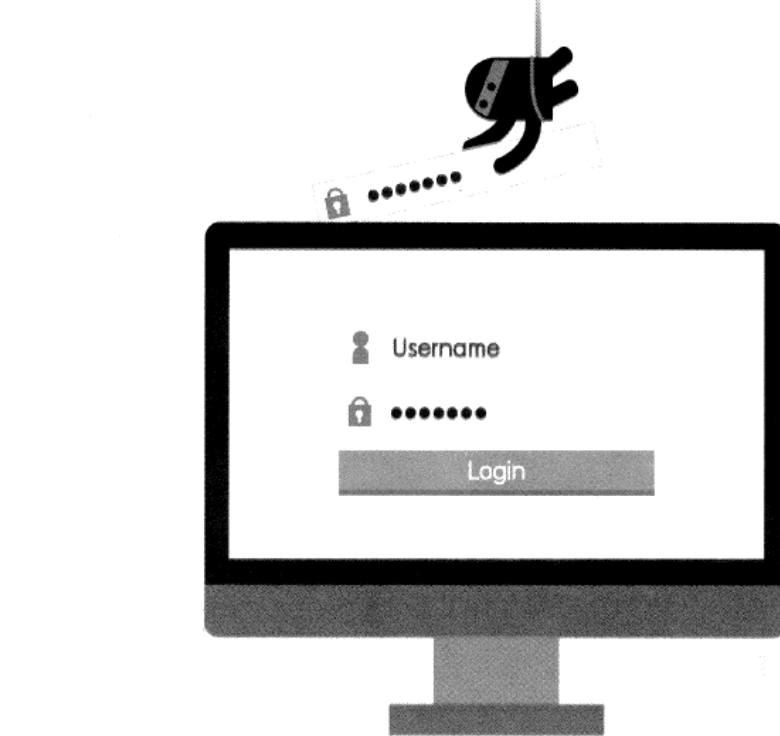
Breaches like these, coupled with the past year's revelations about government data-mining practices, have put us all on alert that our personal, private information might not be as private as we'd like. And, of course, the more information we share, the more vulnerable we become.

Santa Clara County's government, for example, administers social service benefits, delivers healthcare, and assesses and collects property taxes, just to name a few of its duties. To do this work, agencies collect personal and financial information from county residents and often store it for years out of legal necessity. Valley Medical Center alone holds records for roughly 450,000 people.

The county has a lot of personal information that is and should stay private. What it does not have yet, however, is a comprehensive set of policies and procedures for handling and protecting that information.

State law requires companies and government agencies to disclose privacy breaches to affected parties. But far better than disclosure after the fact is working to prevent the breaches from occurring in the first place.

The county has been working to create a privacy and data protection policy that builds on the good work being done in individual agencies. That means collecting only the information we really need, limiting access to that information, protecting that information with the best available technology and creating a privacy culture throughout the county organization. It means privacy has to be a front-end consideration, not an after-the-fact realization.



THINKSTOCK



Joe Simitian chairs the Santa Clara County Board of Supervisors Finance & Government Operations Committee, and is the past chair of the California State Senate Select Committee on Privacy.

Comprehensive privacy protection is not easy – or the county would already be doing it. In mission-driven government agencies,

taking time and resources away from core duties to implement privacy measures can be seen as a distraction, as well as a cost. If you're a doctor, you want to save lives. If you're a cop, you want to catch bad guys. Too often, privacy is an afterthought.

But I think it's vital. When your privacy is compromised, your safety, your assets and your reputation are all at risk. Like taxpayer money, this information is fundamentally yours. Our job in the public sector is to be responsible stewards.

If you agree, let your elected officials know. Tell them you expect them to do the public's business with a commitment to protecting the public's privacy.

The Mercury News

February 26, 2015

Editorial

County needs more privacy protections

One of the biggest issues confronting Silicon Valley is privacy concerns over the tech industry's most innovative and revenue-generating products. The future of Apple's iPhone, Google's search engines, Facebook's posts and a multitude of other applications hinges on the public's trust that their rights will not be abused.

Santa Clara County should therefore be among the first to explore the efficacy of new tools for law enforcement and craft intelligent policies and ordinances for their use in the most transparent manner possible.

The Sheriff Office's effort to obtain a portable cellphone tracking system failed that test in practically every way possible.

Supervisor Joe Simitian summed it up best Tuesday before being the only dissenting vote on the board's decision to go ahead with the purchase:

"Just to be clear," he said, "we're being asked to spend \$500,000 of taxpayers' money, plus \$40,000 a year for a product the brand name of which you are not sure, the specs you don't know, a demonstration for which you haven't seen for which there is no policy in place, for which you have a nondisclosure agreement."

The only thing Sheriff Laurie Smith was able to articulate well at Tuesday's board meeting was the potential benefits of the device (the video of the board discussion is available at the 36th minute on the county website: <http://bit.ly/1zJv5XY>).

The Sheriff's Office

(cont. next page)

could use the cellphone tracker to locate missing persons — including children and seniors with some form of dementia — human trafficking victims and high-level felons. Sgt. Kurtis Stenderup pointed to several high-profile cases in recent years in which the device could possibly have saved lives. It's not difficult to understand the attraction of the tracker, which impersonates a cellphone tower to identify the use of cellphones within its range.

Smith insisted that it would only be used after a warrant had been granted or in the type of typical emergency situations for which policies already dictate sheriff's Office actions. She also maintained that the device could only be used to track specific

cellphone numbers. That's where potential objections arise. Privacy experts challenge that assertion, saying the device can be used to track other cellphones and also capture emails, texts and conversations.

The Board of Supervisors rushed to approve the request because of the imminent deadline for winning the \$500,000 federal grant. The silver lining in agreeing to craft the rules for use after its purchase is that it allows the board to dictate an airtight ordinance the Sheriff's Office will be forced to follow.

The goal should be to deliver an ordinance that protects county residents' privacy and serves as a model for other counties throughout California and the nation.

December 19, 2017

Santa Clara County Hires Its First-Ever Chief Privacy Officer

By **Jennifer Wadsworth** @jennwadsworth/ December 19, 2017



Mike Shapiro comes to the county with experience in both the public and private sectors, where he trained government agencies and corporations on data breaches and program development.

Santa Clara County appointed its first privacy chief, U.S. Army veteran and security expert Mike Shapiro. The Board of Supervisors announced his hire at a subcommittee meeting Thursday.

Supervisor Joe Simitian pushed the county this year to establish the nation's first Privacy Center of Excellence, and said hiring a chief privacy official was the logical next step.

“Santa Clara County, as a government, collects sensitive and personal information, including health, financial, voting, and criminal records,” Simitian said in a press release about the new hire. “With Mike Shapiro on board, I’m hopeful that we can become a national leader—in not only protecting that information from outside assault, but in handling it appropriately within the County.”

Shapiro comes to the county with experience in both the public and private sectors, where he trained government agencies and corporations on data breaches and program development.

(cont. next page)

In his first report to the county's Finance and Open Government Committee last week, Shapiro and Chief Information Security Officer Justin Dietrich listed ongoing efforts to improve privacy aspects of policies on surveillance, whistleblower protections, patient confidentiality and data sharing.

Shapiro said he's eager to help the county build a robust privacy program, which could set an example for other local governments. Developing Simitian's vision for a Privacy Center of Excellence will require balancing personal privacy with the benefits of information sharing, Shapiro said.

"I'm ready to use my skills to create an enterprise privacy program in support of constituent and employee privacy alike," Shapiro said in a statement.

He added: "We're in Silicon Valley, and in our unique region, we have the ability to work with academia and the tech industry on the most urgent privacy threats and solutions."

This county is apparently one of the few in the U.S. with a dedicated chief privacy officer. Some states don't even have one yet, noted Shapiro, whose hire is part of a longstanding effort by Simitian to bolster privacy protections. According to his office, the supervisor sponsored 12 privacy-related laws in as many years in the California legislature. Simitian also chaired the Select Committee on Privacy in both the Assembly and the state Senate.

Simitian introduced what became the country's first data breach disclosure law, which requires companies to notify affected customers if their information is compromised. He also co-authored legislation that required website operators that collect sensitive information to clearly post and abide by a privacy policy.

When Simitian came back from Sacramento to local government, he led the county to adopt transparency rules for surveillance technology, including law enforcement tools such as cellphone towers, computer hacks, license plate scanners and GPS trackers.

Jennifer Wadsworth is the former news editor for San Jose Inside and Metro Silicon Valley. Follow her on Twitter at @jennwadsworth.