

A green banner advertisement for Workopolis. On the left, the 'workopolis' logo is in green with a bar chart icon, followed by the text 'IS NOW HIRING: INSIDE SALES EXPERTS'. In the center is a green button with white text that says 'CLICK HERE TO APPLY'. On the right, a hand is holding a white card that reads 'reason #28 5% EMPLOYER RSP CONTRIBUTIONS'.

Smart grid saves power, but can it thwart hackers?

August 03, 2009

TYLER HAMILTON

The illegal access of 179,000 Toronto Hydro e-billing accounts last week may be written off by some as just another privacy breach in an increasingly interconnected world, but it also raises a red flag in the rush toward the "smart grid."

Customer information taken in this case included names, addresses, customer account numbers and some billing information, all building blocks for anyone serious about committing identity theft. "Nobody knows if it was a rogue employee or somebody else. It's a big question mark," says Ann Cavoukian, Ontario's information and privacy commissioner, in an interview.

To its credit, Toronto Hydro was quick to act. But Cavoukian, who is investigating the breach, sees it as a wake-up call of sorts as utilities begin to modernize their networks and embrace communications technologies to better interact with customers.

She mentions Google and its plan to work with certain utilities – Toronto Hydro included – to demonstrate its new residential energy management tool, Google PowerMeter. Are the proper policies in place, for example, to make sure your personal information as a customer is protected when it's handed over to Google?

"There needs to be a wall between Toronto Hydro customer information and Google being able to take that and connect it with other information Google possesses that may be linked through your Gmail account," she says. (Disclosure: I co-authored a book on data privacy with Cavoukian in 2002)

Her concern could just as easily extend to Microsoft and its new energy management tool, Hohm. Or the dozens of similar, much more advanced applications that will use two-way broadband and wireless networks to gather customer data, including energy use, for highly detailed analysis and feedback.

"The smart grid is a good idea, and I'm certainly in favour of it. But the focus is so much on controlling energy use that I think the privacy issue is a sleeper; it's not top-of-mind," Cavoukian says.

That was the same message heard Friday at the Black Hat security conference in Las Vegas. That's where Mike Davis, a security consultant with IOActive Inc. in Seattle, showed how someone could hack into a smart meter and install a computer worm that could spread to other smart meters used by homes and businesses connected to a local distribution hub.

The worm, apparently, could have been programmed with the ability to take over the meter and remotely disconnect someone's power. Davis was able to demonstrate this

under contract with an unnamed utility, which hired him to test smart meter security. He told his audience the general attitude among utilities is "We'll fix this later," and privacy and security aren't being taken as seriously as they should.

This raises many questions. Could a hacker remotely spread a virus through smart meters and then disconnect power from thousands of homes and businesses? If so, it could introduce tremendous instability to the grid.

There are already conservation programs in Ontario that give a utility the ability to remotely shut off or control air conditioners, water heaters and other appliances when required to reduce the load during peak times. General Electric said last month it will offer in 2010 a "home energy manager" that can connect with and control appliances and a "smart" thermostat in the home. Could someone with malicious intentions gain access and wreak havoc?

On an individual household level, knowing hourly energy use can help thieves. If, over a few days, the load appears flat, it can tell a burglar you're on vacation and nobody is home to catch you breaking in.

"We're doomed to relive the 1980s and 1990s all over again," says Davis, referring to the hard security lessons learned by banks, retailers and others when computers became more networked and the Internet emerged onto the scene.

Stuart Brimley, manager of training and emergency preparedness at Ontario's Independent Electricity System Operator, says utilities didn't have to worry as much in the past because their computer systems were all closed-standard, proprietary systems and therefore less vulnerable to attack. "As an industry we've been lucky historically. But that's changing," he says.

Brimley says the big fear is that the grid – from the customers that use power to the companies that generate it – is going to have more points of access that increase vulnerability. At the transmission level, this cyber security risk isn't lost on the North American Electric Reliability Corporation, or NERC.

NERC has mandated that big utilities and system operators comply with eight standards related to infrastructure protection, including physical and cyber security. "Right now, cyber security standards in place today only apply to a dozen different companies here in Ontario," says Brimley. "The move to the smart grid expands that to many, many companies, every single distributor of power across Ontario."

Brimley says in his 10 years focusing on this area, he's had high-level access to intelligence information and there has been little indication terrorist organizations or rogue states have tried to attack power grids in Canada. In April, however, the *Wall Street Journal* reported cyber spies had penetrated the U.S. grid and planted malicious software that could potentially cause disruptions. It's conceivable that as an evolving smart grid sees more points of access and vulnerability emerging, Canada could become an attractive entry point for disrupting our neighbour.

"There is no border when it comes to electricity," says Brimley, "and it's the same with the cyber threat."