Netwatch

BY JIM CARROLL

YOUR GUIDE TO BUSINESS & ACCOUNTING ON THE INTERNET

Of groundhogs, criminals and hackers

I spent much of my summer at war with a groundhog. My efforts were spectacularly unsuccessful, until I figured out how he was working. He first destroyed our vegetable garden, which I dutifully fenced off with garden mesh and boards. He proceeded to dig under this obstacle, leading me to establish a second, inner barrier of chicken wire and sticks. That worked — the garden became groundhog-free. That is, until he dug a huge burrow under my patio deck. I countered with pressure-treated 2x4s sunk in concrete, along with wire and other defence mechanisms. He went on to attack another area. Fortunately, I got wise to his ways and moved in with a pre-emptive defence system. My family must think I've lost it.

Maybe so, but the anticipatory approach to those with a nefarious purpose is a good strategy for protecting your assets. This brings me to the issue of policing and law enforcement, which is much like battling a groundhog. The police deal with unique challenges that constantly change, whether fighting white-collar or street crime.

I recently spoke to chiefs from several hundred municipal, provincial and federal police forces on this theme, noting that a key focus for law enforcement must be the rapid ingestion of new technologies to deal with the ingenuity of those they are up against.

Through the next decade, police forces will start using sophisticated technologies such as clothing that will link to an in-car mapping system through a wireless network, allowing officers to perform a "hot-location" lookup of a colleague in the field during a ground operation. We'll see today's current generation of military hardware become a part of tomorrow's crime-fighting infrastructure, such as unmanned aerial drones being used for highway surveillance to crack down on street racing. Police education will change as well, with a migration toward virtual reality training based on airline simulator models.

Then there's the world of financial crime. Certainly today's financial criminals are adept at using technology to cover their tracks, whether it be with encryption, underground payment networks or sophisticated document manipulation software. Investigators must stay on the leading edge of technology so they can keep up with the increasing scope and complexity of financial crime.

The same holds true for financial professionals, whose jobs involve continually assessing the risk, management strategies and control infrastructures for emerging technologies. Consider, for example, the concept of contactless payment technologies. In the near future, your cellphone, BlackBerry and other handheld devices are likely to include embedded technology that will become a part of our national payment infrastructure. You'll pay your gas bill simply by swiping your cellphone past the pump.

While such a development brings new opportunities for more efficient financial systems, it also brings a new element of risk. It would only be a matter of time before a sophisticated criminal group figures out how to modify the code within the device to alter the identity or increase an embedded financial value. Various global websites that explore how to hack such new payment technologies might emerge, much as we witnessed a group of Apple fanatics learn about various ways to hack the new iPhone.

As financial professionals, we need to keep on top of new technologies that come at us full throttle, and move into a proactive mindset that ensures we put in place appropriate defence mechanisms within our organizations. Just like I've been trying to do with that darned groundhog.

Jim Carroll, FCA, is a well-known speaker, author and columnist. Reach him at jcarroll@jimcarroll.com or log on to his website at www.jimcarroll.com

DEFENDING YOUR ASSETS

Police Futurists International
www.policefuturists.org

Predictions of a "Groundhog Day" of garden damage http://landscaping.about.com/cs/pestcontrol/a/groundhog_day.htm

iPhone Hacks www.iphonehacks.com