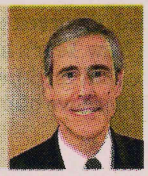
Know how companies protect us from cyberattacks

SPOONFUL OF SUGAR

BY RICHARD A. SUGAR:
Serving tastings of money, taxes and the law



This past holiday season, I had a hard time choosing appropriate gifts for my family. Everything I looked at seemed to be tied to the Internet — a Kindle, a smartphone, an iPad, a Netflix subscription, a new home monitoring service, a new garage door with remote connectivity, a GPS, a subscription to U.S. News & World Report. But something bothered me about all these gifts. I kept having nightmares about all the cyber-intrusions of 2014 — Sony's computers, Target and Home Depot credit cards, JP Morgan/Chase's banking network. They reminded me of the vulnerability we all experience when we go online. And it is hard to escape going online today. So I wondered, how can we protect our security, our identity, and our money?

For one thing, the Department of Homeland Security offers some advice (on its website, of course) in an article entitled "Protect Myself from Cyber Attacks:"

Never click on links in emails and never open attachments; instead go directly to the vendor's website.

Never give out personal information over the phone or by email. Instead, call or email the vendor directly.

Set secure passwords and don't share them.

Keep your operating system, browser, anti-virus, and other critical software up to date.

On a web page titled "Consumer Information 7 Protecting Your Identity," the U.S. Federal Trade Commission suggests I purchase identity theft protection coverage and warns me about how to do that.

But even if I do all those things, how will that protect me if a government agency, seller, or service provider gets hacked and my information is stolen? What is government and industry doing to keep my personal information safe?

It turns out efforts have begun. In 2011, the US Securities and Exchange Commission (SEC) issued a directive that required public companies to disclose to the public, in their filings, the cybersecurity risks they face and the preventative actions being taken to address those risks. In late 2013, the International Organization for Standardization (ISO, the world's largest independent non-governmental membership organization made up of 165 member countries today) issued a series of standards for managing, evaluating, and upgrading information security management systems, and permitted users to be audited and certified. More recently, the National Institute of Standards and Technology (run out of the US Department of Commerce) issued its first draft of a "Framework for Improving Critical Infrastructure Cybersecurity" in early 2014. The publication does not have the force of law, but rather offers a scientific approach for financial, energy and health care companies, as well as those in other critical areas, to protect their information and physical assets from cyberattack.

It seems to me my shopping would have been so much simpler if I could easily find out (probably online) which companies had taken approved measures to keep my personal information safe, and that of my family, when I buy them internet-connected gifts. But since I couldn't find such a resource, I just resorted to buying — for cash — scarves, earmuffs, and gloves at bricks and mortar stores.