AMERICAN BANKER
THE FINANCIAL SERVICES DAILY

Bank Think
VIEWPOINT: Make Security Motivating

By **Anne Wallace**
467 words
25 January 2011
American Banker
AMB
8
Vol.176, No.13
English

Computer security professionals are to meet at the RSA Conference next month to figure out how to protect our citizens and enterprises from cyberattacks. I suggest they start thinking more like marketing professionals and answer a threshold question for consumers, "What's in it for me?"

If people knew the consequences of poor security habits, they might act differently. But our experience is that, though consumer education is vital, it only goes so far. People are more likely to change their behavior after something bad happens, not before.

Consumer electronics companies are masters at understanding human behavior and creating products that anticipate and respond to human wants and needs. The most successful devices, and the applications that support them, are indispensable to their owners. By understanding how we behave today and what we will want tomorrow, Apple, Motorola and Research In Motion create compelling relationships between device and user.

The smartest processes, and the best technologies, are not effective if people do not want to use them, avoid them or will not update them. Technology and processes depend on user adoption and consistent use to be effective. This appears to be the Achilles heel in our current approach to cybersecurity.

Is it crazy to suggest that we create new gadgets and technologies for security that are appealing and that people will want to use? It must be possible to design a technology that delivers such obvious value that people will want to have a relationship. I admit it is hard to imagine consumers lining up for the latest version of MyCyberSecurityBlanket the way they did for the iPad, or downloading the latest security app the way they downloaded Angry Birds, but shouldn't that be our inspiration?

We know that understanding human behavior is fundamental to addressing cybersecurity. In a report presented to Congress in 2009, the Institute for Information Infrastructure Protection recommended research into developing a security culture that incorporates insights into human behavior. Specifically, understanding what motivates bad actors, why victims of cybercrime perform bad actions, making security intuitive and therefore easy for individuals and putting security in the context of how and where it is being used.

Researchers are building behavior-based security protocols, for example, examining the principles of anthropology in relation to security, including the role of rituals in human behavior. Other research involves conferring human characteristics on our machines, such as biometric "pets" to authenticate an owner's identity or machines that can read human emotion.

Recruiting citizens to the war on cybercrime. The industry must develop and market tools that are easy-to-use, intuitive, unobtrusive and maybe even emotionally rewarding.

Maybe there will be an app for that in 2012.

Anne Wallace is president of the Identity Theft Assistance Center.

Document AMB0000020110125e71p0000f

