I agree with the recommendations included in the Cybersecurity Green Paper. Even though they are voluntary they may serve as an informal “minimum standard” for internet security policies . Today’s policies are far too disparate which causes users to have numerous password formats, etc. to deal with each entity. Many are far too weak to be effective and even more are far too difficult for everyday users to implement. Standardization, in terms of a minimum acceptable level, would facilitate having policies that are more closely aligned and raise the effectiveness and usability of systems.

These standards should also be specific to the types of threats that organizations typically experience. For example, phishing seems to be the favored method of attack for online financial transactions. In such situations static passwords, no matter how complex, are ineffective. The recommendations here should include things like one-time passcode generation systems or bio-metrics as the primary defense.

Alignment of security standards that provide the greatest security and usability by area of use could help provide overall focus in internet security while reducing the number of things that users have to possess or remember.

Given the rapid rate of change in IT, these standards would have to be revisited in relatively short intervals, possibly as little as six months, to insure that they remain relevant.

Also, I like the idea of providing financial incentives to organizations that meet the minimum standard. In my experience, as unintuitive as it may seem, organizations are often unwilling to spend to upgrade their security levels even though the ROI could be short and substantial. A program of financial incentives could help them overcome short term budget constraints.

Regards

K.A. (Ken) Kotowich
President
It’s Me! Security