MOVEMENT IN THE RIGHT DIRECTION ON CYBER SECURITY

While the bulk of mainstream news coverage on cyber issues has been focused on macro issues such as Russian involvement in our electoral process, there have been less noted initial signs of progress on the more traditional cyber concerns such as the protection of critical infrastructure, theft of intellectual property and securing of personal data.

The most encouraging signs can be found in the draft Executive Order on cyber that floated into the community last Friday. While much of the draft order addresses organizational and timing issues the Trump Administration is considering, the most encouraging elements of the draft can be found in the direction the Order suggests the new Administration will take when addressing the cyber threat. I'm focused on what questions will the new team be asking as they develop policy, because if you ask the wrong questions you get the wrong answers.

My reading of the draft suggests the Trump team maybe asking the right questions.

Specifically, the Order seems to suggest that the Trump team may view cyber less simply as an "IT issue" and more as system wide problem that has as many economic aspects as it does technical ones. In particular the draft order requires an analysis of private sector incentives for infrastructure development.

While the Obama Administration paid lip service to addressing the incentives for cyber security, even including it in EO 13636, in truth there was very little work done either in the Congress or Executive branch on cyber incentives. The notable exception being enactment of the CISA information sharing bill, which used liability protections to incentivize increased information sharing. I'm aware of only one hearing in either body of Congress that has even examined the issue of cyber incentives, and that hearing was a decade ago.

Yet understanding the complicated, and in many ways upside-down, nature of digital economics, and rebalancing the incentive structure for cyber security, is critical to creating a sustainably secure cyber system.

ISA published an extensive treatment of this issue this past fall (see The Cybersecurity Social Contract) but the cliff-notes version of the economic balance between attackers and defenders in cyber space is the following:

On the attack side, cyber attack techniques are comparatively easy and inexpensive to access, the profits that can be generated from cyber attacks are enormous (current estimates of losses are in the hundreds of billions and heading toward the trillions), and the business plan is excellent (you can use the same techniques over an over on a world wide basis)

On the defender side we have to protect an inherently insecure system that is getting technically weaker every day due to things like IoT and mobile device explosion. Our defense techniques are almost endemically a generation behind the attacker. Its hard to show ROI for things you have prevented and we get almost no help from law enforcement –we successfully prosecute maybe 1% of cyber attackers (and by the way this is not law enforcement's fault – they are also dealing with outdated structures and are vastly under resourced).

And that is just the cliff-notes version. Cyber security economics becomes even more complicated when we add in second order issues such as interconnection, nation-state support for criminals (and its not just the Chinese and Russians), scarcity of trained personnel, an outdated legal framework, the inadequacy of traditional risk assessment models, and – heaven help us – governmental and regulatory turf wars.

Also, it seems as many of the cyber criminals are pretty savvy business people who are wisely reinvesting their profits to build the business and innovating new techniques including finding new vulnerabilities in the core protocols the Internet is based on. They are also generally "exempt" from regulation.

So, if the Trump Administration is going to include a serious analysis of the economic incentive structures affecting cyber security as they begin to develop policy, I see that as not only progressive, it's visionary.

Moreover, even leaving aside direct financial incentives such as tax breaks or grants, the reality is that we have multiple other creative incentive structures built into various sectors of our economy such as pharmaceuticals, aviation, environment, agriculture that potentially can be adapted to the cyber security problem. Existing government levers such as regulatory forbearance, procurement, good actor preferences, liability protections, and insurance can be applied much more creatively to the serious and growing cyber problem.