Happy New Year: We Need a New Approach to Cybersecurity

January 2, 2018
By Larry Clinton

We all know we are losing the battle to secure cyber space – badly. Maybe our New Year's resolution ought to be to recognize this fact and come up with a new approach to the problem. The old ones don't seem to be working.

Specifically, we should consider moving away from our current approach, which focuses on securing various critical assets connected to the network to one that recognizes that cyber risk is systemic risk and, thus, we need to focus more on securing the system itself rather than just incremental assets.

THE GOOD

To be fair, we have had some successes in the cybersecurity field. For one thing, we are at least aware of the problem. October, Cybersecurity Awareness Month, is probably anachronistic. Pretty much, everyone knows we have a cybersecurity problem; cyber understanding is a different story. We also have achieved a bipartisan approach to addressing the issue. Operating in an intensely partisan environment, cybersecurity is one of the few areas of political consensus, recognizing we need a creative partnership. Properly defining that partnership is still undone.

Corporate boards also have now been activated. Just a few years ago, cyber ranked outside the top ten concerns for boards and now it routinely polls as one of the top 3 issues – sometimes number one – boards much face. This has been reflected in increased spending and systemic improvements. Congress enacted a visionary incentive-based information sharing bill that is beginning to show results, the NIST Framework is increasingly being used, and the federal government is modernizing their infrastructure and even taking steps to adopt a more digitally-based organizational structure.

THE BAD

Still, hardly a day goes by without notice of a successful hack. Loss estimates run from the billions to hundreds of billions of dollars and up. Nation-states have expanded their cyber operations beyond traditional espionage to straight out cyber-crime, like bank robbing. It seems no one is safe – just last month the NSA and the U.S. Army were successfully compromised.

Perhaps most worrisome, attack techniques are becoming so accessible that rogue states and terrorists, unfettered by the interdependent economics that constrain major powers, may soon pose serious risk to critical infrastructure.

Frustrated by almost constant reminders that the attackers are running up the score on us, we too often hear the same blame-the-victim bromides we have heard for a decade. To some, the answer to this extremely complicated problem is simple (i.e. we need greater "accountability," fire the CIOs, fire the CISOs — hell, fire the CEOs, and replace the boards – off with their heads).

It's never too clear who we are getting to replace these people. And, I wonder, are we also firing the leadership at the recently compromised NSA and U.S. Army? They are the "A-Team." I'm not sure we have an A+ team in the cyber minor leagues ready to be called up.

THE UGLY

The ugly truth is we still are mostly underestimating and over-simplifying the issue. The dominant narrative is that the victim entity was just stupid. "If only this one patch had been downloaded to modify this compromised vulnerability, the attack would never have occurred," is a common theme.

According to this narrative, our core problem is that we have stupid, probably lazy, sometimes corrupt, no doubt money-grubbing people running our cybersecurity (apparently at the NSA and U.S. Army too – who knew?).

Purveyors of the "one simple patch" theory of cybersecurity seem not to appreciate the "P" word in the now common cyber term "APT." It stands for Persistent. It means that modern attackers – and nowadays APT can just as easily stand for average persistent threat – continually probe targeted systems until they find an opening. Often these attackers are nation-states or nation-state affiliates – Kevin Mandiant has been quoted as saying 90% of the attacks he sees are nation-state affiliated. The reason the attackers are so persistent is that the profits from a successful attack, ranging from virtually priceless IP to our top military secretes, is so great.

For effective security, you don't need to just download that one simple patch; you need to download all the patches and promptly – not as easy as it may sound. And, as our Target friends discovered, you also need to not only download all your patches, but those of your air conditioner vendor – and all your other vendors.

WHAT'S THE PROBLEM?

We no doubt do have some stupid, lazy, whatever, people involved in cybersecurity – we do everywhere else, I'm sure cyber is no different. But that is not our main problem.

However, the main problem is that we have a fundamentally vulnerable system protecting immensely valuable data. It's not that individual organizations are vulnerable, it's that the system itself is vulnerable. This systemic risk is a different – and more difficult – problem than managing incremental risks for a particular asset or organization.

Moreover, technical innovation, like mobile devices and the Internet of Things, are making the system even weaker. On top of that, it turns out the bad guys are pretty good business people who are wisely reinvesting their enormous profits back into the business and finding new vulnerabilities we didn't know were there.

The reality is that cyber targets are increasingly being vastly out gunned by the attackers. Although "providing for the common defense" is the very first obligation of the government under the U.S. Constitution, our government has failed to define a clear policy, strategy or structure to effectively assist private companies in fending off well-funded nation-state (or state-affiliated) cyber attacks.

NEW YEAR'S THINKING ABOUT CYBERSECURITY

Cyber breaches are not like historic corporate malfeasance, such as Enron and WorldCom. In those cases, government needed to protect consumers from corrupt companies. However, in the cyber world, consumers, government and industry are all being attacked. We are all on the same side. We need to act like it.

Government policy, structure and funding needs to be substantially enhanced in order to carry out their Constitutional mandate to provide for the common defense and promote the general welfare in the digital age. How to do so needs to be developed through a conscious partnership process similar to that which NIST conducted in developing the operational Cybersecurity Framework, but this time targeted at the strategic level and addressing the real systemic threats. (ISA has offered a 12-step program in our "Cybersecurity Social Contract" which may be a place to start).

We also need to evolve from historic security models wherein we expect each entity to secure itself. The Internet is a distributed interdependent system and we need to evolve an interdependent system of security. We need to move way beyond critical, but operational, tactics such as information sharing. And we need to evolve a system that fits within our understanding of democracy and free markets that will sustain the innovation and productivity, which are the foundation of our culture.

We have a lot to think through. Good thing we have a brand-new year to get started.

Larry Clinton serves as the President and CEO for the Internet Security Alliance.