Petya Provides Context for Briefing Council on Foreign Relations

It appears the dust was just settling from the global impact of the WannaCry ransomware attack when a new culprit Petya (or not Petya) struck. Among the disturbing characteristics of these attacks is their vast international impact.

Desperate for a silver lining, this happens to be a great backdrop for my previously scheduled briefing digital policy experts at the Council on Foreign Relations on June 29. However, the silver lining ends there. The reality is that things are liable to get worse – much worse – before they get better. One has to wonder how many wake-up calls we need (Target, Sony, OPM, Yahoo and on …) before we stop hitting the snooze button.

Maybe it will help if instead of just saying things will get worse we explain why this is path we are on. I'll offer four reasons. First, the system, which of course, was designed to be weak (open), is getting weaker with the explosion of mobile devices and the Internet of Things. In addition, the bad guys turn out to be fairly good business people and are reinvesting in their business including finding all new vulnerabilities we didn't even know about.

Second, the attackers are getting better. Nation-states are now engaged in traditional criminal behavior including the recent ransomware attacks, which like Sony and Bangladesh can be traced to North Korea. They are literally funding their military buildup with cybercrime. And the traditional criminals are getting as good as the nation-states making previously advanced-style attacks commonplace. APT should now stand for Average Persistent Threat.

Third, all the economics of cyber favor the attackers. Attacks are cheap and easy to acquire (Petya was available wholesale on the Dark web) and yield tremendous profits. Meanwhile, defenses are generations behind the attackers while defending an inherently vulnerable system, with little help from law enforcement. We successfully prosecute maybe 1% of cyber criminals. Finally, terrorists are getting much better at cyber-attacks and could become a much more substantial, and scary, threat in the near future.

Are we making any progress? Yeah, a little. Corporate boards are becoming much more involved in cybersecurity activities and some programs that are being adopted are showing positive results. This is in large part due to new thought leadership that is being spread amongst the cybersecurity community, such as NACD's recently published, in cooperation with the Internet Security Alliance and AIG, Cyber-Risk Oversight Handbook for Corporate Boards. In addition, we actually have developed a fairly broad consensus on the best ways to approach and address cyber public policy. Leaving peripheral issues aside, the House GOP, the Obama Executive Order and the Trump Executive Order all pull in much the same direction.

But every great plan eventually devolves into actual work and we need to really get to work. I will present the same 12-step program ISA's offered in our Cybersecurity Social Contract, released last fall and available on Amazon. Briefly, ISA believes government needs to 1) Address the problem with greater urgency, 2) Spend (a lot) more money, 3) Focus more on law enforcement, 4) Reorganize government for the digital age, 5) Streamline cyber regulations, 6) Develop effectiveness measures for the NIST Cybersecurity Framework, 7) Train senior

government executives in cyber risk management, 8) Adopt a true risk management approach at federal agencies, 9) More creative workforce development, 10) Define government's role in nation-state attacks, 11) Realign cyber market incentives, and 12) Rethink the cyber compliance model.

That's a lot of work but it's not impossible. Wait, I think I hear another wake-up call.

Written by Larry Clinton, ISA's President & CEO