CyberPro

November 3, 2011

Keeping Cyberspace Professionals Informed

Senior Leader Perspective: Larry Clinton, Internet Security Alliance

Larry Clinton is President of the Internet Security Alliance (ISA). ISA is a multi-sector trade association with membership from virtually every one of the designated critical industry sectors. The mission of the ISA is to combine advanced technology with economics and public policy to create a sustainable system of cyber security.

Mr. Clinton is known for his ability to take the complicated issues in this space and explain them clearly to a wide range of audiences---professional, policy makers and the general public. He has been featured in mass media such as USA Today, the PBS News Hour, and the Morning Show on CBS, Fox News, CNN's Situation Room, C-SPAN, and CNBC. He has also authored numerous professional journal articles on cyber security. This year he has published articles in the Cutter IT Journal, the Journal of Strategic Security and the Journal of Software Technology.

Mr. Clinton is regularly called upon to testify before both the U.S. House and Senate. In 2008 ISA published its Cyber Security Social Contract which is both the first and last source cited in the Executive Summary of President Obama's Cyber Space Policy Review, which also cited more than a dozen ISA's white papers –far more than any other source.

The ISA's pro-market, anti regulatory approach to cyber security is outlined in its numerous publications including the ISA Cyber Security Social Contract and the Financial Management of Cyber Security which were written by the ISA Board of Directors and edited by Mr. Clinton.

NSCI: What is the focus of the Internet Security Alliance?

CLINTON: The Internet Security Alliance was founded in 2000 in collaboration with Carnegie Mellon University. It is a multi-sector trade association. The membership includes major corporate entities representing most aspects of our nation's critical infrastructure including aviation, banking, communication, defense, education, financial services, health care, insurance, manufacturing, and security and technology companies.

The mission of the ISA is to integrate advanced technology with economics and public policy to create a sustainable system of cyber security

NSCI: Many have talked about a potential "Cyber Pearl Harbor," specifically as it relates to a major cyber attack on our critical infrastructure. How real would you say this kind of threat is?

CLINTON: Our nation's critical infrastructure has been under cyber attack all day, every day, thousands of times a day and this has been the case for several years. Despite this constant status of defense, there is not one single case of a successful cyber attack that led to a loss of life, disruption of a critical infrastructure, or denial of access to critical national security resources. It is certainly possible that a devastating attack is in our future, but we must acknowledge that nearly 20 years of unrelenting attacks have produced no successes at the Pearl Harbor level for our adversaries. We are doing something right, and we need to give credit to those in the private and public sectors who continue to protect our nation's critical infrastructures, systems, and services.

That said, it is also important to realize we are seeing a paradigm shift with respect to the sophistication and purpose of these attacks. Ultra sophisticated attacks, sometimes called "APT" attacks, that a few years ago were concentrated in the government and defense sectors are now spreading throughout our critical infrastructure necessitating a rethinking of our defense strategies. Most of these attacks seem designed not to take down our systems but to use them as a vehicle to steal intellectual property and business processes. Moreover, whereas a few years ago most cyber attacks were fairly benign, we are now seeing attacks such as STUXNET which is specifically designed to take down critical infrastructure

Attacks are becoming more sophisticated and widespread and multi-purpose, and thus the need to evolve and create ever more dynamic systems to defend ourselves.

NSCI: You've had the opportunity to speak to many audiences including the U.S. House and Senate, Fox News, CNN, and others. What are the top 2 or 3 questions you get, and how do you answer them?

CLINTON: Probably the question I get asked most often in these forums is what should the government be doing about cyber attacks and do we need government regulation in this space.

I think there is an important role for government, although it may not in all instances be the traditional regulator role we have come to expect.

We have to realize it is not so much that our systems are defective; it's that they are under attack, which is a very different thing. The APT style attacks I mentioned before are not hackers or kids in basements. These are highly organized, well funded, usually state supported professionals who launch so many ultra sophisticated attacks at its target that it will breach the system. This doesn't mean we have no defense, but it means the notion of perimeter defense defined by some government mandated standard is primitive and outmoded for most cases.

Regulations can be used in industries where the economics are baked into the regulatory model or for things like consumer protection and awareness, but in general traditional regulation is not well suited to fighting cyber attacks. The technology and attack methods change too quickly for regulators to keep up with via a regulatory process. US regulations only reach to US companies and the problem is clearly international and regulating technology will inhibit innovation and investment which we can't afford.

ISA has advocated that we need a 21st century solution to a 21st century problem. We need a "Cyber Security Social Contract" between the government and the innovators who own, operate, and create the technology we are now dependent on. We have articulated this model in some detail, but, in short, we believe the government's role in this model is to evaluate the effectiveness of various methods independently and motivate, via market incentives, their voluntary adoption. Industry's role is to innovate and implement solutions that are both technologically successful in managing risk and economically sensible so that they can be maintained.

NSCI: How would you characterize the right balance between government regulation and policy as opposed to allowing the market to lead cybersecurity improvement?

CLINTON: Markets don't spring magically in full form out of Adam Smith's invisible hand. They are created, managed and evolved. In general, the market has done well in creating mechanisms to deal with cyber threats. Multiple studies have all concluded that somewhere between 80-95% of cyber attacks could be prevented or fully mitigated simply by adopting standards, practices and technologies the market has already created.

It's not that we don't know how to deal with our cyber security problem; it's that we don't want to pay for it. Multiple studies have also concluded that the biggest single barrier to improved cyber defense is cost. The reason we have so many cyber attacks is the incentives all favor the attackers. Attacks, even ultra sophisticated ones, are comparatively cheap compared to the enormous profit they can yield. Moreover, they are fairly easy to obtain and criminal prosecution is almost non-existent despite herculean efforts from a badly over matched law enforcement community.

Although the cyber threats are rising dramatically, investment in cyber security has been going down for several years. We all know we are in a historic period of belt tightening and so we have to find a way to make investments that are currently deemed uneconomic. Traditional regulation actually increases costs for compliance but does not yield improvements in security. Indeed, the increased focus on compliance actually subtracts from already underfunded security budgets and is anti-security.

We have proposed greater use of the incentive programs we have historically used in other areas of the economy (e.g. environment, agriculture, transportation) and apply these incentives to cyber security. Many of the incentives that will drive increased private investment in cyber security do not cost the government significantly to implement; things like liability reform, procurement reform, better use of insurance, streamlining regulation, expediting permitting etc. Government should be offering this menu of incentives for organizations that are willing to make otherwise uneconomic investments in cyber security that go beyond their business model but address broader national security concerns.

NSCI: What key policy and legislative gaps do you see regarding our nation's ability to defend against and respond to cybersecurity threats?

CLINTON: Our current policy apparatus and many of the legislative policy proposals are set up to fight the last war. They tend to focus on perimeter defense, under the assumption that if you take reasonable care you can stop cyber breaches. That is a faulty assumption.

Private firms defending against APT attacks are basically fighting the Chinese government. They are in over their head. After all, Google got successfully breached---as has the federal government. Dick Clark says this is like if in World War II the pentagon had gone to US Steel and told them they thought the Germans were going to bomb their plants in Pennsylvania so US Steel better buy some anti aircraft weapons and radar.

There are elite private organizations who, like sophisticated government experts, can do a great deal to assist us in collective cyber defense but we are keeping these people in silos apart from each other rather than finding a way to bring them together to develop solutions that can be sent out to the rest of the population that is never going to be able to fight the APT by themselves.

We need collaboration, not regulation. Regulation will generate an adversarial process geared to minimal compliance on politically watered down regimes. It will be like campaign finance---everyone will say they comply and everyone will know it's meaningless.

The private sector has made a range of proposals to move in this direction, but we have yet to see them enacted.

NSCI: With so much to do, where do you think the current administration should focus their cybersecurity efforts?

CLINTON: The Administration should start by getting its own house in order. The WikiLeaks fiasco from earlier this year was emblematic of the lax approach to cyber security. In that case, a poorly supervised employee with a Lady GaGA CD was allowed access to masses of highly classified data and released it on the Internet. That was not a sophisticated APT attack but a simple case of poor management resulting in a massive cyber leak. And the annual FISMA scores measuring government adoption of its own standards are an embarrassment.

In addition, the government has not adapted their structures for dealing with the private sector; resulting in confused and overlapping authorities that lead to costly and redundant procedures draining needed resources for our cyber security efforts.

Government needs to lead by example.

NSCI: The Department of Defense recently conducted a pilot project that included sharing threat information with the private sector. Should we see more of this type of information sharing? Any thoughts on other ways to increase information sharing between the public and private sectors?

CLINTON: As a cross sectoral organization with many DIB members ISA is looking into the adaptability of the DIB process to other critical industries. However, it's worth noting the DIB has some real unique characteristics compared to other portions of the economy.

On the broader issue of how to improve information sharing we have proposed a different model that would bring elite government and industry players to share different information. Most attacks are not successful when they breach a system; they are only successful when they break back out with the payload data they are trying to steal. If we focus on sharing information about the command and control centers receiving this data we might be able to lock the thief "in the vault", thus compromising the attack's effectiveness. In addition, since we no longer are looking to share source information or corporate processes ---as is often the case now---we should have a much more amenable process both industry and government can feel more comfortable with.

NSCI: What are the top 2 or 3 technology challenges you think we need to solve to have a more secure internet??

CLINTON: I guess the top challenge is that the Internet was designed to be an open system and not with security in mind. To a large extent we are still using this same open system.

The second technological challenge is the incredible proliferation of mobile devices and social media which are being brought into the enterprise space and integrated with core networks. This is adding whole new dimensions of complexity to enterprise risk management problem we face with cyber security.

NSCI: Lastly, what would you consider ISA's greatest success(es) to date and what should we expect to see in the future?

CLINTON:

ISA has historically taken a slightly different view of cyber security from the mainstream. We have never viewed it a primarily a technological problem (although obviously it has massive tech dimensions) but we have seen it as an enterprise wide risk management issue. Consistent with this is the notion that the economic and public policy issues are just as important to resolve as the technical ones. That was the basis of our Cyber Security Social Contract.

We are now seeing these ideas incorporated into the mainstream. The Executive Summary to President Obama's Cyber Space Policy Review both begins and ends by citing the ISA. Our white papers and other documents filling out these ideas are cited 4x more than any other source in the President's signature document on the subject.

Traditionally, the "partisan divide" in cyber security is between the vendors and the users (and maybe the civil libertarians). Yet this Spring we were able to bring together major trade associations representing the major vendor's providers, both hardware and software, and the major user associations along with the civil liberties community on a detailed white paper that also embraces the concepts in the ISA Social Contract.

Then, the House Republican Task Force Report on Cyber Security, published earlier this month, also relies heavily on the ideas in the ISA Cyber Social Contract lifting many of our proposals virtually verbatim and recommending them as the appropriate path forward.

We are also seeing our enterprise educational programs like the “50 Questions Every CFO Should Ask About Cyber Security” and “The Financial Management of Cyber Risk” being cited and used as the basis for corporate education programs being provided by major, non-ISA affiliated vendors.

And of course our organization has basically tripled in size in the last 3 years, so our members are voting with their pocketbooks in favor of our efforts.

NSCI: Is there anything else you’d like to add?

CLINTON: Thank you very much for this opportunity

NSCI: Thank you very much for taking the time to visit with us.