Enhancing and Implementation Cybersecurity Elements of Sector Specific Plans

House Homeland Security subcommittee on Emerging, Threats, Cybersecurity, Science and Technology

Testimony of Larry Clinton, Internet Security Alliance
October 31, 2007

Good Morning, I am Larry Clinton, President & CEO of the Internet Security Alliance (ISAlliance). I also am a member of the DHS's Communications Sector Coordinating Council, the Critical Infrastructure Partnership Advisory Council and serve as an Officer on the IT Sector Coordinating Council.

ISAlliance is a cross-sector trade association focused exclusively on information security. We were created in 2001 as collaboration with the Carnegie Mellon University. We now have roughly 1,000 member companies. We provide our members with a range of services, including technical, business operational and public policy. ISAlliance provides its members with an integrated series of security services addressing the technical, legal, business and public policy concerns simultaneously.

I want to thank the Chairman for inviting me to participate.

ISAlliance continues to believe that the threat to our economy, our nation, and our citizenry from cyber attacks is real and growing.

We also believe that government and industry must work much more aggressively to address these threats. We are past the time for simple education about the cyber threat. Now is the time for action.

However, for industry and government to create a sustainable and effective system of cyber defense we need a fundamental re-thinking of how we go about addressing these issues.

This rethinking must include at least three critical realizations.

First, the Internet is a technology unlike anything we have dealt with before and hence will require a solution unlike what we have traditionally used to address technology and business.

We need to change the way government, perhaps including Congress, thinks about and conceptualizes its role in assuring Internet security. In its June 2006 report, "Internet Infrastructure: DHS Faces Challenges in Developing a Joint Public/Private Recovery Plan," the GAO got it right. It listed as the number one challenge we face the "innate characteristics of the Internet."

How then is the Internet different?

- It transmits phone calls but it is not a phone line.
- It makes copies but it is not a Xerox machine.
- It houses books but it is not a library.
- It broadcasts images but it is not a TV station.
- It is critical to our national defense, but it is not a military installation.
- It is all these things and much, much more.

The Internet is international, interactive, constantly changing, constantly under attack, then changes and changes again.

It is not even really an "It." It is actually lots of "Its" all knitted together--some public, some private--all transmitting information across corporate and national borders without stopping to pay tolls or check regional sensitivities.

We can not simply "cut and paste" previous governance systems from old technologies or business models and realistically expect that we will be able to manage this system effectively.

The regulatory model we have traditionally used to govern business has not changed much since we created it to deal with the breakthrough technology of 2 centuries ago---the railroad.

To manage the railroad, Congress decided to create an expert agency, the ICC, to pass specific regulations. The ICC begat the rest of the alphabet soup: the FCC, the SEC, the FTC. And, that system has worked arguably well in most instances.

But that system will not work with Internet security. Even if Congress were to enact an enlightened statute, it would not have reach beyond our national borders and hence would not be comprehensive enough. Even if some agency wrote a brilliant regulation, it would likely be out-dated before it got through the process, a process that can be further delayed with court challenges.

And that assumes, unrealistically, that the political process inherent in a government regulation system doesn't "dumb-down" the eventual regulations so that we wind up with a campaign-finance-style standard where everyone can attest that they met the federal regulations, but everyone knows the system is really not working.

That may work in politics, but, frankly, we can't afford that when it comes to Internet security.

Regrettably not enough is being done, either by government or industry, to secure cyber space. We have attempted to manage the risk of first 21st century technology solely using regulatory models designed two centuries ago. While regulation has its place, a new, more creative, model built on market incentives must be developed.

Yet, we can't stand idly by either. We must, together, develop a mechanism to assure an effective and sustainable system of security that will accommodate the global breadth of the Internet and still result in a dynamic and constantly improving system of mutual security.

Second, information security is not a static technical problem. Even within the past couple of years the threats have become not just more sophisticated, but more subtle.

For example, we now know that threats to the net have morphed from broad and often relatively benign, if well publicized, attacks like Love Bug and Blaster, to designer malware constructed to target specific systems where it can reside undetected by traditional methods for an indeterminate period of time while causing serious damage.

As a result, traditional AV software and firewall solutions are becoming inadequate. However, a new generation of security products has been, and continues to be, developed to address the continually evolving threats.

To adequately address information security concerns we need to address the full organizational system which relies on information infrastructure.

Our members now look to us to provide a comprehensive risk management approach that encompasses the full-system approach necessary to address the problem. An example is our Enterprise Integration Program which addresses discrete cyber security issues ranging from preventing and handling breaches of personal information to securing the IT supply chain in the era of globalization.

We address these issues by looking at their technical, business operational, human resource, legal and public policy aspects simultaneously and developing an integrated solution. We would commend this fully integrated model to our government partners to consider.

Third, the threat to this nation's and the world's economic infrastructure from the risk of cyber-attack is real.

Two years ago ISA reported to this Committee that the main protocol used to protect this data is over 30 years old and has multiple well-know security flaws.

Since then the massive growth in Internet use based on these same protocols has increased the vulnerability of the Internet at a massive rate.

In addition there are now far more attackers and they have become increasingly more sophisticated. Whereas only a few years ago "hackers" created cutely named attacks like the "love bug" and "slammer" largely to get attention, the current generation use stealth and designer malware that is difficult to detect and in some cases virtually impossible to eradicate.

Even worse, the motivation for Internet attacks is no longer publicity, but money, and more insidiously power and destruction.

Especially worrisome are the cyber-attacks that would hijack systems with false information in order to discredit the systems or do lasting physical damage. At a corporate level, attacks of this kind have the potential to create liabilities and losses large enough to bankrupt most companies. At a national level, attacks of this kind, directed at critical infrastructure industries, have the potential to cause hundreds of billions of dollars worth of damage and to cause thousands of deaths.

Some of the attack scenarios that would produce the most devastating consequences are now being outlined on hacker websites and at hacker conventions. The overall patterns of cyber intrusion campaigns suggest that a number of potentially hostile groups and nation states are actively acquiring the capability to carry out such attacks. Meanwhile, the many ways in which criminal organizations could reap huge profits from highly destructive attacks are also now being widely discussed.
Forth, There is some good news. We actually know a good deal about how to protect the Internet.

The best evidence of this is that although the Internet is under attack constantly---thousands of times a day ----it has yet to fail. The owners and operators of the Internet, primarily the major private sector players are doing a terrific job managing the defense.

Major independent surveys, such as the PricewaterhouseCoopers "Global State of Information Security" ---the largest study of its kind--- have indicated that those entities that follow approved best practices of information security show a remarkable ability to fend off attacks, recover from attacks and even deter attacks.

The problem is that as the Internet continues to grow we need more entities to embrace these practices and technologies while also working with us to develop new ones.

The critical question is: how precisely can we create such a system, if the models we have used for previous technologies are inadequate?

The best mechanism to assure an adequate and sustainable defense system is to inject market incentives to motivate the adoption of best practices.

That has been the mantra of the Internet Security Alliance, and The National Infrastructure Protection Plan officially embraced the need for a government supported market based incentive program stating that the "Government can … [create] an environment that supports incentives for companies to voluntarily adopt widely accepted sound security practices"

Fifth, there is a concrete proposal for moving forward.

The ISAlliance has long campaigned for the development of a publicly supported market based incentive program to bridge the gap between a regulatory and pure volunteer approach.

ISAlliance believes that the Federal government should advance homeland security preparedness through reliance on existing published standards *and best practices*, and defer to the private sector to continue to invest in and develop appropriate general and industry-specific standards for improved security.

Fortunately, there exist a number of paths, most with Congressional precedent, for Congressional action to provide incentives that are in the national interest. Among these paths are:

1. Congress can use its market power, instead of its regulatory power by more prominently including security, along with cost into its procurement process.

2. Congress can lead by example by fully funding federal agency needs for cyber security and integrating security compliance into personnel evaluations along with other HR criteria

3. Congress can tie incentives such as civil liability safe harbors such as those provided in the Safety Act, or provide procurement credits to companies who can demonstrate compliance with market generated best practices for cyber security;

4. Congress can stimulate the stunted cyber insurance market by temporarily sharing the risk of a massive cyber-hurricane until the market is sufficiently large to take the risk themselves.

5. The Congress can create an industry/government/university consortium to stimulate the needed research, development and adoption of security protocols, similar to the Sema-Tech model used in the late 1980s to address the computer chip gap.

6. The Government can create awards programs similar to the "Baldrige Awards" for quality which eventually became a sought after market differentiator for corporations.

Earlier this year the Board of Directors of the Internet Security Alliance met and approved an outline for a legislative approach we offer for your considerations which we call the "Cyber-Security Safety Act of 2007." I spend the balance of my statement further detailing our thoughts on how the Saftey Act can be used as a model for improved cyber security.

We do not come to the Committee with legislative language which we are endorsing, but rather with a set of concrete policy proposals we urge the Congress to work with us on perfecting.

We believe the "Cyber Safety Act" offers a coherent approach which will create specific Federal support for a package of incentives that will affirmatively encourage private sector investment in improved security and protection of the Internet. I would like to use the remainder of my testimony to outline he specific incentive recommendations and offer a brief analysis in their support:

- Establish a mechanism which will enable companies that adopt standards-based information security programs or best practices to be qualified to receive the specified incentives ("Qualified Companies").

  The availability of incentives requires some type of baseline as a criterion to be met for the incentives to be available. The ISAlliance has long advocated that private sector standards and best practices are already in place that can be adopted by DHS as a basis for incentives.

- Create, in connection with privacy reform legislation (such as uniform breach notice laws), a Federal limitation of liability for Qualifying Companies that would limit their liability for breaches that occur, notwithstanding their use of standards-based security and best practices.

  Information security is closely associated with privacy protection. Many companies otherwise eligible to be Qualified Companies have large volumes of personal information requiring protection under various Federal and state laws. Those companies will not be motivated to move forward with their cyber-security investments if they still are exposed to liability when breaches occur notwithstanding good security practices. As a final piece of the litigation-related incentives, this incentive eliminates the inhibitor of continued privacy-related liability for Qualifying Companies.

- Establish Federal Acquisition Regulations (FARs) and other legal frameworks through which private sector companies do business with the United States government that:

  Require the agencies to specify published standards and best practices as required elements for any contract relating to information security, data protection or similar services.

- Qualified Companies should be able to acquire additional cyber-security insurance to cover losses arising from CINS-related catastrophic events, and limit their liability to third-parties to the amount of that insurance. The amount of the insurance acquired must be reasonable in order to qualify for the limited liability.

  Many companies defer investments in improved security out of a concern that, even with improved security, they are not protected from liability for losses that occur despite the quality of their security controls. Businesses are encouraged to invest in becoming Qualified Companies when they are offered the protection that is provided by a) assuring the availability of insurance to cover losses from CINS-related catastrophic events and b) limited their liability to the amount of insurance that has been obtained.

  The principles of limiting liability to encourage improved homeland security are similar to the structures used to incent new homeland security technologies under the SAFETY Act which was enacted as part of the Homeland Security Act of 2002.

- To support the preceding insurance market, the Federal government should create within DHS a national program for temporary, short term reinsurance, through which insurers may purchase reinsurance coverage for their exposure to CINS-related catastrophic losses under policies issued to Qualified Companies.

  Insurance carriers have been reluctant to create a vigorous marketplace for cyber-security insurance. The chief reason is that the insurance companies lack sufficient experience with cyber-terrorism to effectively evaluate the overall risks in order to determine effective premium levels, particularly for CINS-related catastrophes.

The proposed established of a reinsurance program provides underwriting for the insurance companies. In the event losses are incurred by the purchasing insurance carrier is greater than their reinsurance deductible, the insurer would be entitled to coverage under the reinsurance agreement with the Federal program. The program administrator would have the right to increase future reinsurance premiums as deemed necessary to accomplish a revenue neutral goal. Over time, the program could be sunsetted as the insurance market gains experience with cyber-security coverage. This solution is similar to Federal legislation that enhances the airline transport industry.

- Qualified Companies with appropriate insurance will also have litigation-related incentives available, excluding liability for consequential and punitive damages and limiting their liability for non-economic losses.

  Similar to the incentive provided by a limitation on losses to the available insurance, the limitation of liability for consequential and punitive damages, and limited liability for non-economic losses removes a serious inhibitor to information security investments—i.e., the risk of losses for which responsibility is assigned notwithstanding a company's good faith investments in adequate information security. Eliminating that inhibitor encourages a more secure preparedness, company-by-company.

  On many occasions, the Federal government has employed its influence as a major purchaser from the private sector to encourage companies to develop and implement improved business practices. Establishing criteria tied to providing services to the government offers new market opportunities to Qualified Companies and, in doing so, provides strong economic incentives to improving their cyber-security.

- Establish a "Baldrige Award" for information security quality and excellence, coordinated with specific industry organizations to develop and create awareness of information security as a competitive differentiator.

The Malcolm Baldrige Award by the US Department of Commerce has become a cherished recognition of excellence in the marketplace. A similar program, perhaps recognizing information security excellence within industry sectors, will greatly increase awareness of the value of information security and its function as a competitive differentiator, thereby encouraging new investments.

- Create and fund an industry/government/university consortium to stimulate the needed research, development and adoption of security protocols that can, in turn, stimulate improved technologies for adoption across the private sector and government computer systems.

  In the late 1980's, the Federal government provided matching funding to create an industry-government cooperative consortium that collaborated in accelerating solutions to common manufacturing problems in semi-conductor production (SEMATECH). This successful model revitalized the U.S. semiconductor industry and continues to generate industry leadership and innovation long after Federal funding was voluntarily terminated by the consortium.

  A similar program today will enable government, academia and industry to work together to replace today's security poor Internet protocols with security-rich protocols. Those protocols can enhance the quality and integrity of the hardware devices, switches and other components from which the Internet is constructed.

<u>The bottom line is this Mr. Chairman:</u>

We have major security issues revolving around the Internet

If we attempt to use traditional regulatory methods as the sole means to address these threats we will be unsuccessful in the long run

The federal government in cooperation with the private sector can create an effective and sustainable security in cyber space by supporting market based incentives.