TESTIMONY

LARRY CLINTON
PRESIDENT, INTERNET SECURITY ALLIANCE

WHAT GOVERNMENT CAN LEARN FROM THE PRIVATE SECTOR ON CYBER SECURITY

JANUARY 8, 2016

Mr. Chairman let me put this simply. We are not doing enough to combat the growing cyber threat, and what we are doing we are not doing nearly fast enough.

THE NEED FOR US TO WORK BETTER TOGETHER

The core question of today's hearing -- what can the public sector learn from the private sector -- is an excellent question.

Not only **can** we learn from each other, we **need** to learn from each other. Moreover, we need to be working together much more effectively

AT LEAST WE ARE ON THE RIGHT PATH -- JUST MOVING TOO SLOWLY

To be fair there has been progress -- learning -- at least at the broad policy level. Just a few years ago both Republicans and Democrats were offering legislative proposals on cyber security that basically tried to adapt a traditional regulatory model to the cyber problem as if we were dealing with a simple consumer product safety issue that could be solved. That approach would have failed miserably.

In 2009 the ISA produced the "Cyber Security Social Contract"[1] that described why the traditional regulatory model not only wouldn't work, but would be counter- productive to enhancing our security and offered a different approach. The Social Contract model proposed that government and industry work together to identify effective standards and practices and that voluntary adoption of these standards and practices ought to be motivated via a system of incentives.

In 2011 a broad spectrum of the private sector including the ISA, US Chamber of Commerce, Tech America, the Business Software Alliance and the Center for Democracy

---

[1] http://isalliance.org/publications/2B.%20Social%20Contract%202.0%20-%20A%2021st%20Century%20Program%20for%20Effective%20Cyber%20Security%20-%20ISA%202010.pdf

and Technology embraced the social contract approach in a comprehensive whitepaper on cyber security.[2]

In 2012 the House GOP Cyber Security Task Force appointed by Speaker Boehner and Chaired by Mac Thornberry listened as all 5 private sector organizations supported this model and in the end the GOP Task Force endorsed this approach. [3]

In 2013 President Obama, reversed his earlier government centric regulatory approach and also listened to the private sector. He then issued Executive Order 13636 on cyber security[4] which similarly embraced the Social Contract approach and directed the National Institute on Standards and Technology (NIST) to develop the framework of cyber standards and practices and directed federal agencies to determine what incentives could be offered to promote voluntary adoption of the NIST Framework.

The recently enacted information sharing legislation is an example of this approach. It does not mandate information sharing with the government -- as for example does the current EU proposal does -- but motivates voluntary sharing by offering a liability incentive. This approach has received bi-partisan support in the Senate and is supported at least conceptually by the Administration.

A related example of the federal government listening to the private sector with respect to information sharing has to do with the information sharing mechanisms and their need of reform. Again harkening back to the ISA's 2009 Cyber Social Contract document and the subsequent multi-trade association white paper of 2011, the private sector argued that the historic sector-by-sector structures of information sharing were inadequate and inefficient.

From a cyber security perspective large defense contractors probably have more in common with large financial institutions than with small banks and "mom and pop" component suppliers within their so-called sectors. More importantly, the existing structures were primarily attuned to the needs and processes of larger institutions leaving small and mid-sized players largely as non-participants in information sharing programs. A far more effective structure would be cross-sector information sharing especially among the major players with economies of scope and scale who could then manage the sophisticated information they can generate and analyze amongst themselves and pre-digest it into actionable elements for smaller players.

---

[2] http://isalliance.org/publications/2C.%20Industry-Civil%20Liberties%20Community%20Cybersecurity%20White%20Paper%20-%20Improving%20our%20Nation's%20Cybersecurity%20through%20the%20Public-Private%20Partnership%20-%203-2011.pdf

[3] http://thornberry.house.gov/uploadedfiles/cstf_final_recommendations.pdf

[4] https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

Once again the government has listened. In February of this year President Obama signed Executive Order 13691[5] that seeks to expand the current "ISAC" model and spur the development of broader "ISAOs" many of which will operate across the sectors and specifically design programs to make cyber information shared more timely, digestible and actionable for the smaller organizations who we now understand are not only targets in their own right but conduits to larger elements of the critical infrastructure. DHS has initiated a grant process to establish a standards organization to facilitate the development of these new, more modern information-sharing entities.

These positive steps to enhance our nation's cyber security are an outgrowth of the policy makers listening to and learning from the private sector, which has greater experience with, and understanding of, the cyber security problem.

This listening model needs to be followed and expanded and we congratulate the Committee for being supportive of that effort.

10 LESSONS THE GOVERNMENT CAN LEARN FROM THE PRIVATE SECTOR

1. The government needs to invest more on cyber security.

For the past two years, the United States Worldwide Threat Assessment has listed cyber-attacks above all other threats to US national security – including terrorist and nuclear threats from the middle-east[6]. Director of National Intelligence James Clapper has told Congress "We must be prepared for a catastrophic large-scale cyber strike. We've been living with a constant and expanding barrage of cyberattacks for some time. This insidious trend will continue. Cyber poses a very complex set of threats, because profit- motivated criminals, ideologically motivated hackers, or extremists in variously capable nation-states, like Russia, China, North Korea, and Iran, are all potential adversaries, who, if they choose, can do great harm.[2] Likewise, a recent survey of worldwide stakeholders from the financial services industry ranked cyber risk as by far the single biggest risk to broader global economy.[7]

While the cyber threat to the United States continues to increase in severity and scale of impact, a disparity exists between federal and private sector spending on the issue.

---

[5] https://www.whitehouse.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari

[6] http://www.dni.gov/index.php/newsroom/testimonies/209-congressional-testimonies-2015/1175-dni-clapper-opening-statement-on-the-worldwide-threat-assessment-before-the-senate-armed-services-committee

[7] http://dtcc.com/~/media/Files/pdfs/Systemic-Risk-Report-2015-Q1.pdf

According to the Ponemon Institute, total private sector spending on cyber security (not just IT) has doubled in the past few years and now exceeds $100 billion annually. Federal spending on cyber security is about $13 billion and nearly half of that goes to the military that is largely offensive oriented cyber programs, which, while vital, are not security in the sense we are discussing it today.

That leaves about 6-7 billion dollars a year to fight a problem that experts estimate is costing us many hundreds of billions of dollars, maybe a trillion dollars a year in lost value of IP, business practices and data ---leaving aside the national security risks engendered by private sector losses through cyber means.

I know of two banks that have a combined cyber security budget of $1.25 billion. The DHS cyber budget ---to manage securing the entire civilian government and critical infrastructure is about 900 million ---75% of what just two banks spend.

Meanwhile, the US is spending $95 Billion dollars a year combatting terrorist threats in the middle-east[8] The US spends around $52 Billion dollars[9] a year on our nuclear weapons program and $15.5 Billion a year on securing our southern border[10]

To use Department of Homeland Security spending as a reference, barely 2% ($1.25 Billion) of DHS total 61 Billion dollar budget allocation for fiscal year 2015 is dedicated to cybersecurity activities. DHS spends nearly $6 Billion on immigration issues and $7 Billion is allocated to TSA respectively.

No one is saying these expenditures are not important. However, if our own threat assessment says cyber is the number one threat costing us hundreds of billions of dollars a year, threatening the economic vitality and personal privacy of millions of Americans every day and potentially threatening our national security --- is it logical that our spending on it should be less than half what we are spending on the southern border and one tenth of what we are spending on nuclear which our own official threat assessments rate currently as lower risks? [11]

While the percentage increases in federal cyber spending may sound impressive ---up 35% in the last 3 years ---they are perhaps misleading due meager baseline spending up until very recently. The absolute dollar amount being spent on cyber security in relation to the size of the problem is nowhere near adequate.

---

[8] http://fas.org/sgp/crs/natsec/RL33110.pdf

[9] http://carnegieendowment.org/2009/01/12/nuclear-security-spending-assessing-costs-examining-priorities/8uq

[10] http://www.cbp.gov/sites/default/files/documents/FY2013%20Summary%20of%20Performance%20and%20Financial%20Information%20-%20FINAL%20%28panels%29%20%20%20.pdf

[11] http://www.dhs.gov/sites/default/files/publications/FY15BIB.pdf

Pricewaterhouse predicts privet sector spending on cyber security will increase 24% this year. Federal spending is going up roughly 10% a year.

Cybercrime costs our nation about a half trillion dollars a year. Yet we successfully prosecute about 1% of cyber criminals.

The spending on cyber law enforcement is an excellent example. Multiple independent studies have concluded that the financial losses being suffered by American citizens and businesses -- often at the hands of nation-state affiliated attackers who are using cyber attacks to prop up their domestic economies -- runs to the hundreds of billions of dollars each year.

Yet we are spending maybe one tenth of one percent of that amount to capture these criminals. Our valiant law enforcement officers are fighting the good fight but are hopelessly out matched in terms of overall resources and personnel ---and the attack community is investing at a much higher rate than we are on the law enforcement side where we are fighting to achieve incremental operational increases.

2. The Government must act with much greater urgency on the policy recommendations it claims to have learned from the private sector

While we are naturally pleased to see the number of hearings Congress is now holding on cyber security issues, the fact remains that it took Congress 6 years to pass a fairly modest information sharing bill.

The House GOP Task Force on Cyber Security made its legislative recommendations including first and foremost the need for Congress to develop a "menu of incentives" to promote a voluntary program of cyber security in 2012. Now more than three years later, apart from the information sharing bill, there is not a single bill I am aware of in the House that follows through on that primary recommendation. Moreover, I'm unaware of a single hearing that has focused on the development of an incentive model for cyber security or even the overall economics of the cyber security issue.

Similarly the President's Executive Order on cyber security was issued in February of 2012. Yet despite some blogging by the White House there has not been a single legislative proposal come forth from the Administration following through on the President's Order to develop a set of incentives to promote voluntary adoption of the NIST Framework.

ISA alone has testified in the House and Senate more than a dozen times over its 15 year history urging that Congress enact meaningful cyber legislation and including a nearly a dozen specific incentive models. The Partnership for Critical Infrastructure Security (PCIS) participating all 18 critical sectors put forth a separate set of recommendations to

the DHS at a conference specifically designed for this purpose, yet we have seen no legislative or Administrative action.

We need the government to listen to this plea

The cyber security problem is far, far, more dire than the highly publicized breaches of personal data -- horrible as they are—and things are getting rapidly worse.

Our cyber systems are getting technologically weaker as the attack community finds new weakness in the Internet's core protocols. As we vastly expand the number of access points to penetrate the system and the attack community is growing increasingly sophisticated as the elite techniques against governments and the military that we used to call the advanced persistent threat is now the Average Persistent Threat being used throughout the economy?

Congress is not moving nearly fast enough to keep up with an expanding threat to our cyber infrastructure that is moving ahead at light speed...

3. Federal Government should educate its top leadership on cyber as the private sector is doing

According to the most recent research, cyber security is now the top concern of corporate boards of directors, surpassing last year's number one issue---leadership succession. It's unknown in how many congressional offices cyber security ranks ahead of leadership succession.

Recognizing the ascendency of cyber security as an issue for corporate boards last year the National Association of Corporate Directors (NACD) asked the ISA and AIG to develop for them the first ever handbook on cyber security for corporate boards.[12]

This publication, which has subsequently been endorsed by DHS and the Institute for International Auditing and many others stresses that cyber security much be understood in a much broader context than simply breach prevention and response. Much like legal and finance considerations there is not a single major business decision before corporate boards that doesn't have a cyber security element to it.

Recently, PWC independently validated the success of this approach, in its 2016 threat landscape report:

---

[9] http://www.isalliance.org/national-association-of-corporate-directors-asks-isa-to-create-best-practices-guide-for-corporate-board-of-directors/

"Boards appear to be listening to the NACD guidance. This year we saw a double-digit uptick in Board participation in information security. Leading to a 24% boost in security spending... Other notable outcomes include identification of key risks, fostering an organizational culture of security and better alignment of cyber security with overall risk management and business goals."

NACD and ISA are now designing full training programs for boards, irrespective of their specific businesses, to understand and appreciate this new reality. Boards are being trained to address cyber as part of the core mission of their business and not relegate it simply to the IT department. Senior leadership must embrace this more comprehensive understanding of the cyber threats practice and instill a culture of security throughout the organization.

The federal government might do well to emulate this approach to cyber security realizing that the single greatest cyber vulnerability is not technical but human. Many in senior government leadership positions are what are often referred to as "digital immigrants" meaning they were not born into the digital world they now inhabit. As we are doing with corporate board's senior government officials may do well to be trained not just to be aware of the cyber threat, but to understand it better.

Many of the common "knowledge" and understandings about cyber security widely accepted by government officials are in fact fallacious. For example it's widely assumed that with public awareness of cyber events the stock market will penalize the companies providing a natural incentive for better security. Policy makers may be surprised to find that in reality the stock prices for such well known victim companies as Target and Sony have soured after their breaches ---an effect that has accompanied many recent high-profile breaches.

Similarly government officials have often spoken of how good cyber security is a partner to profitability. Official government publications ranging from the national Strategy to Secure Cyber Space to DHS's highly promoted "Cyber Security Eco-System" program of a couple of years ago asserted claim. The reality is that many if not most of the technological enhancements that drive productivity, growth, profitability and innovation --- VOIP, cloud computing, BYOD (Bring Your Own Device to work) actually come with substantial security downsides and mitigating these security issues comes at potentially substantial economic cost.

The point being that creating an economically sustainable secure cyber system is not easy and not necessarily pro-economic. Policy makers may benefit from the sorts of structured training programs corporate boards are undergoing to learn how best to manage this enormous risk.

Once government, like corporate, leadership better appreciate the cyber threat they will be in a better condition to make sound policy decisions and just as importantly behave

in a way that models good security. Leadership needs to establish clear lines of authority and responsibility and focus on fundamentals as a foundation for all success. Deploying technology solution on top of a weak foundation will not solve problems, it will create them.

It is not required that Agency leadership become technical cyber experts, however as with the private sector, Agency leadership must realize that in the modern world much, if not all, of their missions have a cyber security component As a result, Agency leaders need to at least be able to ask the proper questions of their staff to assess how well the Agency is managing cyber risk. In this regard many of the tools the private secto4r has developed for its own senior leadership are probably easily adapted to the Agency context.

For example the Cyber Security Handbook for Corporate boards [13] ISA wrote for the National Association of Corporate Directors, provides a set of core principles for senior management to use as well as a variety of basic questions that management can ask to assess issues cyber situational awareness, strategy and operations, and incident response.

One technique a "Cybersecurity Balance Sheet" that identifies, at a high level, the company's cyber assets and liabilities and can provide a scorecard for thinking through management progress in implementing the security system.

Assessing the asset side of the balance sheet might begin with identifying the organization's "crown jewels." This is an important exercise, as it is simply not cost-efficient to protect all data at the maximum level. However the organization's most valued data, be it intellectual property, consumer or client information, financial data etc. needs to be identified. Other corporate data can be similarly categorized as to its relative security needs.

The next step is to discuss the strategy for securing data at each level. This strategy generally involves a consideration of people, process and technology.

At the technology process level there are a range of options available with good research indicating cost-effective methods to secure lower-level data and thus reserve deployment of more sophisticated—and hence costly—measures for the data of higher value.

At the people level it is important to follow leading practices for managing personnel, especially with respect to hiring, in-company moves and departures, and the associated system access permissions. Ongoing cybersecurity training is similarly important, and

---

[13] http://www.isalliance.org/national-association-of-corporate-directors-asks-isa-to-create-best-practices-guide-for-corporate-board-of-directors/

will be most effective if cybersecurity metrics are fully integrated into employee evaluation and compensation methods.

Of special attention is the inclusion of senior and other executive level personnel who are both highly valued targets and often uniquely lax in following through on security protocols.

Turning to the liability side of the cyber "balance sheet," an evaluation could start with a look at the business practices that might create liabilities.

Some obvious risks are created by practices such as purchasing services for an un-trusted vendor and not being conscientious regarding discontinuing access rights promptly at project or employee termination. However, additional liabilities are created more subtly from practices such the explosion of mobile devices carrying corporate data, expanding Internet functionality into nonconventional products (the so called "Internet of Things") or the unmanaged data sprawl ---and accompanying vulnerabilities-- that can be a natural byproduct of the increasingly connected world.

4. Government needs to reorganize for the digital age.

The private sector has increasingly moved away from the model wherein one particular department, typically IT, would have "ownership" over cyber security and more toward an enterprise wide model with multiple departments working together with an independent budget.

Government on the other hand has refused to break through the turf wars that are impeding progress and creating unwanted redundancies which are sapping scarce security resources.

The federal government, including Congress, is burdened with legacy structures and procedures designed for a much slower analogue world. The federal procurement systems are a prime example of this dated process. Virtually every single item the government wants to buy has to be bid on and go through an elaborate approval and procurement process. Not only are these policies cumbersome and time consuming but they are expensive as well. While private companies can quickly acquire what they need to secure their networks government agencies are bound by miles of red tape.
A 2015 study compared civilian federal agencies to the private sector and found the federal agencies ranked dead last in fixing security problems and failed to comply with security standards 76% of the time.

Similarly a slow and ineffective government hiring process drives away the candidates. The Partnership for Public Service report cited earlier also found that "the drawn out security clearance process is an impediment as in some cases recruits opt to seek

employment opportunities with private industry rather than wait for the long government process to be completed.." [14]

Several of these issues were also outlined in the GAO's 2011 report, but years later the same issues remain.

A Bank of America Merrill Lynch 2015 report stated:

"The US government is still in the process of determining who will have jurisdiction in cyber space. Departments Agencies and Commands are still battling for jurisdiction and funding. The result is a fragmented system muddled with a political agenda which hinders the development of a more secure system."

The problem is not confined to the federal level either. Virtually every state states and many localities are deciding they want to have their own piece of the cyber security turf and thus are enacting unique rules restrictions and regulations. This patchwork of governmental initiatives further depletes private resources without any perceptible improvement to overall security.

5 Government needs to adopt a risk management approach to cyber security

A study published last summer analyzed the audits of software applications and vulnerabilities in the public and private sector over the past 18 months. The study found that civilian federal agencies rank dead last in fixing security problems in the software they build and buy.

The study also examined software security flaws and how often users complied with widely accepted security standards and how often the vulnerabilities were fixed. The study found that overall federal agencies comply with widely held security standards only 24 percent of the time. By comparison the financial services industry rate of compliance was nearly double (42 percent).

The study also measured how often and how quickly software security flaws are fixed after they are found. Government agencies ranked dead last again. The study found that federal agencies patched flaws in their software only 27 percent of the time. In comparison the manufacturing sector ---not generally considered an industry leader in cyber security---fixed their flaws 81 percent of the time.

The reason government does so badly according to the GAO is that government uses a "policy based" approach where agencies check off a list of requirements set by law makers and regulators.

---

[14] http://ourpublicservice.org/publications/download.php?id=504

Auditors and management can look at a checklist of controls and feel good about meeting 120 out of 125 controls. But meeting standards is a measure of investment and policy decisions, not a measure of security effectiveness. At best it is an indirect indicator. It tells you if you have a firm foundation to build on, but does not tell you how well you've built on it.

The prevailing notion in Congress, government agencies, insurance companies, auditors are that all we need to do is follow the standards. It's understandable given the dearth of other comforting measurements in the cyber arena but it is, nevertheless, a dangerous notion. Standards are great to use as a checklist to ensure you haven't forgotten any of the basics, but standards adherence does not equal security. In the end, standards are about what you do, not how well you do it. What will make the difference are the operational processes and staffing that are built around the systems, which implement the standards.

When we make our primary measure of security success a checklist against standards, the result is often investment without commitment. An agency will invest in products that technically meet some aspect of a standard (typically NIST 800-53 or ISO 270001) but fail to staff it with the operational and sustaining labor needed to really take advantage of the security improvements the product will yield.

For example, agencies can meet several NIST 800-53 controls by having firewalls in place. But who is watching the firewall and looking for gaps or inefficiencies? What governance is placed around the privileged functions in a company that "need" to be outside a firewall to get the job done? Who looks at the firewall logs and thinks, "Hmmm. That looks odd. I think I better dig into that some more."

Private companies typically do the same thing but they add to their mix a risk-based approach. With a risk based approach you don't focus just on the predetermined technical check list but also analyze at what the attackers might want due to current threat indicators and what's in place to stop them. Both approaches are valid but everyone should do both. Federal agencies mostly just do the checklist.

Although government officials often talk about using a risk management approach to cyber security, the hard data demonstrates that they are not in fact following the forward looking process typically practices in the private sector, much to the detriment of the government's own systems.

6. Government does not adequately assess their cyber security programs.

ISA has been involved in numerous partnership programs with the federal government dating back to before DHS was even born. We participate in multiple Sector Coordinating Councils, We are members of DHS's Cross Sector Cyber Security Working

Group, and I have served multiple terms on the board of the Partnership for Critical Infrastructure Protection and many others. Never once has any federal official reported to us regarding the cost effectiveness of any federal partnership program.

Since NIST is in the jurisdiction of the Science Committee we can use it as an example. In 2012 President Obama charged NIST to develop a cyber security Framework. The President's order specified that the Framework be prioritized, cost effective, flexible and be supported by an incentive structure.

Many of us in the private sector praised the design process for the Framework. But once it was designed the federal government went immediately into wide-scale promotion. No sophisticated private sector entity would design a new product or service and go directly to marketing. You design, and then beta test your product or service with your target audience. Based on your beta test you make modifications and then, only then you promote the product or service.

The government simply skipped over these critical steps. As a result now, two years after the Framework was designed, we don't have a single piece of objective data that can tell us what in the Framework has changed behavior or what impact any behavior changes may have had on improving security.

As NIST is under the jurisdiction of the Science Committee and we would urge the Committee to insist that NIST not rely on politically motivated self-reports but work with the Sector Councils develop objective tests of the Framework's effect on actual security. In the private sector the market generally provides a harsh test to the viability of a product or service. Those products that don't meet consumer demand vanish. The government operates without traditional market forces but it can still use private sector based methodologies for beta testing and cost effectiveness evaluation.

All government cyber security programs ought to be routinely evaluated for their cost effectiveness against specific, previously determined objectives. If a program is not meeting these objectives it ought to be terminated or reformed with its funding going to programs that can be more productive

7. Government Needs to Value People as much as Technology

Well run private sector operations understand the need for, and value of, highly skilled cyber security personnel. Multiple government sources have repeatedly noted the difficulty for the public sector to compete with the private sector for this scares resources which is prima facie evidence that industry places a higher value on these people.

We have already discussed the need for government to dramatically increase its funding of cyber security, but it's equally important that the money that is spent is spent wisely.

One area where the government may be spending its limited funds in a less than optimal fashion is their tendency to focus more on buying technical solutions than on people to operate that technology.

A review just this week in the Washington Post made this exact point when it reported: "After personal information for more than 22 million federal employees and others was stolen, the need for modern technology received far more scrutiny during a series of congressional hearings than the need for skilled people to work it. Search for "cyber" on the Government Accountability Office Web site and you'll find dozens of related documents just this year. But if you ask for a study specifically on cyber talent, GAO will provide one -- from 2011.

Alan Paller of the SANS Institute recently made this very point "Government agencies spend a lot on security but just not correctly. Many agencies are literally bristling with sophisticated tools for detecting and monitoring intrusions and threats but they are mainly watched by personnel who do not know what to do with the data generated by these systems. The tools can find the problem but it's the people who know where to look and what is missing."

In addition to being substantively dysfunctional, government's refusal to spend adequately to attract top quality cyber personnel may actually be costing the government money. An April report from the Partnership for Public Service found that: "As the compensation gap continues to widen, especially for the most talented professionals, the federal government will continue to fall behind, but ironically, private companies not limited by federal pay scales can simply hire away the best cyber security talent and rent it back to the government at a higher hourly rate"[15]

The Report concludes that government needs a master cyber workforce strategy to attract and retain top talent, as without a master strategy in place agencies are operating largely on their own in a haphazard system.

8. Government needs to adopt a more segmented approach to cyber promotion Government's generic education programs lack need to

One of our major problems in cyber security is that we simply do not have enough educated cyber security professionals. Despite developing a better cyber workforce being a consensus goal for nearly a decade we do not seems to be making appreciable progress. This lack of progress is more ironic as cyber security jobs are high prestige and high pay, yet the market has not been properly stimulated.

One problem is that the federal government's approach to the cyber workforce development is generic. For example research demonstrates that school guidance

---

[15] http://ourpublicservice.org/publications/download.php?id=504

counsels has generally very little awareness of cyber security career paths and hence are not channeling promising students into this career option.

A market segment approach needs to be adopted by the federal government so they can more effectively use the funds to be devoted to cyber security workforce promotion. In the private sector target segments are carefully drawn and specific marketing campaigns based on consumer research are designed. The federal government needs to adopt these private sector practices to its cyber workforce development programs.

9. Government needs to leverage the private sector more creatively to create a more effective cyber workforce development. Contemporary institutions such as gaming and ESPN can be leveraged to more effectively reach the millennial target audience

One of the most critical steps we, all of us public and private, who are being subjected to the constant cyber assaults need to do is leverage our resources far more efficiently to create sustainably secure cyber eco-system.

The attack community not only has "first mover" advantage forcing us largely into a responsive mode to novel attack methods, but they are better organized than we are. They are more flexible than we are. They are being more innovative than we are. They have a more efficient and effective financing system than we do.

All the economic advantages in the cyber security eco-system favor the attack community. Attacks are comparatively cheap and easy to access. The attacker worldwide business model is highly efficient. Cyber-attacks are tremendously profitable. On the defense side we are almost inherently a generation behind the attackers. It is difficult to demonstrate ROI to preventing attacks. Consumers, including the federal government, are not putting an appropriate economic value on cyber security --- preferring functionality and low cost-- to security. The interconnected nature of the system exacerbates the vulnerability even of good actors, which could undermine investment. And, there is virtually no law enforcement. We successfully prosecute maybe 1 or 2 percent of cyber criminals.

It is absolutely critical not only for the federal government to learn from the private sector but that it also contributes more effectively to the collective defense effort. One place to start is with more creative education and outreach programs

For nearly a decade DHS has been running an outreach program called NICE which is outdated and lacks needed imagination to reach the generation that will drive effective workforce development.

NICE's slogan, Stop, Think, Connect, is straight out of the dial up age ---millennials, in fact almost no one stops and thinks before they connect to the Internet---we have long been in an age where people are virtually always connected. Millennials often sleep with their smart phones on, connected and receiving.

Instead of NICE, the four letters DHS ought to focus on is ESPN. As is being pioneered in Asian countries the Gaming world is being targeted with tens of thousands of your, tech-savvy players attending tournaments and hundreds of thousand "tuning in" on line.

DHS ought to collaborate with private entities like DHS and find a way to market these programs and blend cyber security elements into the spectacle. Promotions and camps could be provided in partnerships that would capture the joy millennials get from gaming and steer at least a portion into cyber security education and carriers.

10. The federal government needs to treat the private sector like true partners, not stakeholders

Government need to appreciate that with the private sector owning and operating the vast majority of cyber infrastructure, and being subjected to attacks form nation states on private enterprise, the traditional roles for government and industry many not apply in the cyber security context.

Improvements can be made in many areas including tactical, such as more effectively sharing information. However some of the work that needs to be done at a broad conceptual level such as working through a coherent policy for the role of the federal government with respect to assisting the private sector when it is attacked by nation-state or state affiliated attackers.

A useful place to start would be for government to stop blaming the corporate victims of cyber-attacks. The annual report of the Pentagon for 2015 states that most DOD systems are subject to being compromised by low to middling level cyber-attacks. In such an environment it's reasonable to ask what level of security we ought to expect from discount retailers and movie studios. Some cyber experts have claimed that as much as 90 percent of the cyber-attacks they are working on have at least some element of nation state affiliation. James Clapper stated just last month that it is unfair to be blaming these victims in the press when they are fighting off irresistible foes.

At a more operational level government needs to work with industry to create an organizationally coherent cyber eco system wherein trust can be established and we in the defenses community can better leverage our resources in the face of the better organized attack community.

ONE PAGE SUMMARY OF TESTIMONY OF INTERNET SECURITY ALLIANCE PRESIDENT LARRY CLINTON ON WHAT GOVERNMENT CAN LEARN FROM THE PRIVATE SECTOR ON CYBER SECURITY

1. Federal government must invest much more in cyber security. The private sector is investing at a far greater rate with increase rates two and a half times as much as federal non-defense spending. Just two banks spend 25% more than all of DHS
2. Government must act with greater urgency. It took 6years to pass a modest info-sharing bill. Four years after the House GOP Task Force Report on cyber security there has been almost no progress on its top recommendations
3. Top policy makers need to be educated about cyber security. The private sector is educating its top management, such as corporate boards with dramatic policy impact. We need an education program for government equivalents to corporate boards including Members of Congress
4. Government needs to reorganize for the digital age. The private sector is moving to an enterprise wide approach to cyber security. Government is still fighting turf wars which inhibits progress and wastes scarce resources
5. Government needs to adopt a risk management approach to cyber security. Government ranks last in adopting standards and fixing problems because it uses check list security instead of risk management as the private sector does
6. Government needs to assess its own programs for cost effectiveness. Unlike the private sector programs like the NIST Framework were not beta tested so we have no objective data as to their actual effect on improving security.
7. Government needs to focus more on people as opposed technology. Government tends to be over reliant on tech solutions to cyber problems while the underinvestment in people undermines the effectiveness of tech
8. Government needs to adopt a more segmented approach to cyber promotion Government's generic education programs lack need to be segmented and targeted similar to the process the private sector uses
9. Government needs to leverage the private sector more creatively to create a more effective cyber workforce development. Contemporary institutions such as gaming and ESPN can be leveraged to more effectively reach the millennial target audience
10. Government needs to treat the private sector as true partners and not as government stakeholders. The blame the victim orientation of many government agents needs to be reoriented to create a more effective partnership

BIOGRAPHY

LARRY CLINTON
PRESIDENT, INTERNET SECURITY ALLIANCE

2500 Wilson Blvd., Suite 245
Arlington, VA 22201
lclinton@isalliance.org
703-907-7028

Larry Clinton is President and CEO of the Internet Security Alliance (ISA), a multi-sector trade association focused on cyber thought leadership, policy advocacy and promoting sound security practices for corporations. In 2015 Mr. Clinton was named as one of the 100 most influential individuals in the field of corporate governance by the National Association of Corporate Directors (NACD). He is widely published on cyber security and was the principle author of the Cyber Risk Handbook for Corporate Boards published by NACD in 2014 and endorsed by DHS in 2015. He has been featured by WSJ, USA Today Fox News, NBC, CBS, NYT, PBS Morning Edition CNN & MTV. He testifies often before Congress; He has briefed industry and governments world-wide including NATO and the OAS. Mr. Clinton was the principle author of the ISA Cyber Social Contract which outlined a market based, as opposed to government regulatory model, for improving cyber security. The document's recommendations were adopted by the House GOP Task Force on Cyber Security in 2012 and it is also the first and most often cited, reference in President Obama's principal policy paper on cyber security. In 2013 the President's Executive Order on cyber security adopted the ISA's market incentive "social contract" model to promote national cyber security.