Larry Clinton
President & CEO
Internet Security Alliance
lclinton@isalliance.org
703-907-7028
202-236-0001
www.isalliance.org

Cloud Commitment

"Current information technology environment is characterized by low asset utilization, a fragmented demand for services duplicating systems environments which are difficult to manage and long procurement lead times. These inefficiencies negatively impact ability to serve customers. "

- Executive Office of the President, Federal Cloud Strategy, February 8, 2011

Cloud Commitment

"Cloud computing has the potential to play a major part in addressing these inefficiencies and improving service delivery. The cloud computing model can significantly help grappling with the need to highly reliable, innovative services quickly despite resource constraints."

- *Executive Office of the President, Federal Cloud Strategy, February 8, 2011*

INTERNET SECURITY ALLIANCE

Cloud Benefits

- MPS to Zero
- Free computing power
- New Business Models
- New VC assumptions

Specific Government Cloud Benefits

- Save $ 50 billion
- Change Government Ops—telecommuting
- Greater customization for citizens
- Stimulate small business if we can find a FISMA compliant cloud

On the other hand, fear

- Dominant – unfriendly clouds
- When data is everywhere – how do we find it?
- Law Enforcement ?
- Compliance?
- Liability?
- Is this really safe – 62% have “little or no confidence” in the ability to secure assets in the cloud – including 49% who use it

Cyber security fear at the highest levels….

"America's economic prosperity in the 21st century will depend on cybersecurity – it's now clear this cyber threat is one of the most serious economic and national security challenges we face as a nation. It's also clear that we're not as prepared as we should be, as a government or as a country."

- President Obama's Remarks on Securing U.S. Cyber Infrastructure, White House, May 29, 2009

Federal Cyber Fears

"The threat [of cyber war] is increasing in scope and scale, and its impact is difficult to overstate. Industry estimates the production of malicious software has reached its highest level yet, with an average of 60,000 new programs or variations identified each day."

-*James Clapper, Director of National Intelligence testimony before the House Permanent Select Committee on Intelligence, 112th Congress, February 11, 2011*

Federal Cyber Fears

"The next Pearl Harbor could very well be a cyber attack. If you have a cyber attack that brings down our power grid system, brings down our financial systems, brings down our government systems, you could paralyze this country. And I think that's a real potential."

-*Leon Panetta, CIA Director, testimony before the House Permanent Select Committee on Intelligence, 112th Congress, February 11, 2011*

INTERNET SECURITY ALLIANCE

What are they afraid of?

- The Advanced Persistent Threat
- Suxtnet
- Cloud Computing
- Things they don't understand


POLICE

ISA Board of Directors

Ty Sagalow, Esq. Chair, Executive Vice President & Chief Innovation Officer, Zurich North America
Tim McKnight, 1st Vice Chair, Vice President & Chief Information Security Officer, Northrop Grumman
Jeff Brown, Secretary / Treasurer, Vice President, Infrastructure and Chief Information Security Officer, Raytheon

- Pradeep Khosla, Founding Director of Cylab, **Carnegie Mellon University**
- Marc Sachs, Vice President Government Affairs, **Verizon**
- Lt. Gen. Charlie Croom (Ret.), Vice President Cyber Security, Solutions **Lockheed Martin**
- Eric Guerrino, Managing Director Systems and Technology, **Bank of New York Mellon**
- Joe Buonomo, President, **DCR**
- Bruno Mahlmann, Vice President Cyber Security Division, **Dell**
- Kevin Meehan, Vice President Information Technology & Chief Information Security Officer, **Boeing**
- Rick Howard, iDefense Manager, **VeriSign**
- Justin Somaini, Chief Information Security Officer, **Symantec**
- Gary McAlum, Chief Security Officer, **USAA**
- Paul Davis, Chief Technology Officer, **NJVC**
- Andy Purdy, Chief Cybersecurity Strategist, **CSC**
- John Havermann, II, Vice President & Director, Cyber Programs , Intelligence & Information, **SAIC**

ISAlliance
Mission Statement

ISA seeks to integrate advanced technology with business economics and public policy to create a sustainable system of cyber security.

The Internet Changes Everything

- Concepts of Privacy
- Concepts of National Defense
- Concepts of Self
- Concepts of Economics
- Cyber security is an economic/strategic issue as much operational/technical one

Cyber Economy is misaligned

"Economists have long known that liability should be assigned to the part that can best manage risk. Yet everywhere we look we see online risk allocated poorly…people who connect insecure machines to the Internet do not bear the full consequences of their actions (and) developers are not compensated for costly efforts to strengthen code."

- *Anderson and Moore, Information Security, October 2006*

Cyber Security Economics are Skewed

- Responsibility, costs, harms and incentives are misaligned
- Individual and Corporate Financial loss (banks)
- Defense Industrial Base
- Core investment is undermined by edge insecurity
- Enterprises are not structured to properly analyze cyber risk
- Competitive pressure drives toward insecurity

INTERNET SECURITY ALLIANCE

VoIP

"While unified communications offer a compelling business case, the strength of the UC solutions in leveraging the internet is also vulnerability. Not only are UC solutions exposed to the security vulnerabilities and risk that the Internet presents, but the availability and relative youth of UC solutions encouraged malicious actors to develop and launch new types of attacks."

-Internet Security Alliance, *Navigating Compliance and Security for Unified Communication*, 2009

Partners, Vendors & Customers

Business demands are making it much more complicated to secure a corporation's technology environment. Business strategies that enhance customer intimacy and optimize supply chains require companies to connect to vendor and customer networks. While tighter integration with business partners provides clear business benefits, it also means that your ability to defend against attacks depends on your partner's or customer's security capabilities and policies. " Kaplan

Cloud

"Virtualization forever changes how organizations achieve control and visibility over core elements of their environment. Infrastructure becomes logical not physical rendering static perimeter based approaches to security and policy enforcement fruitless. Identities become harder to confirm, simply because there are more of them. Information can replicate and relocate instantaneously in the cloud making it hard to safeguard sensitive data." Proof not Promises, Creating the Trusted Cloud. RSA 2011

What we do know about security is all bad

- All the economic incentives favor the attackers, i.e. attacks are cheap, easy, profitable and chances of getting caught are small
- Defense inherently is a generation behind the attacker, the perimeter to defend is endless, ROI is hard to show
- Until we solve the cyber economics equation we will not have cyber security

Where is the Govt Going? Regulation

"Public-private partnerships, information sharing and self-regulation are remedies we have tried for more than a decade without success. Identifying progress in 2011 will be simple. If the nation passes laws and the administration issues effective regulations for critical infrastructure there has been progress. No regulations mean inadequate progress."

-*Lewis, James, CSIS Commission on Cybersecurity for the 44th Presidency, January 2011*

Congressional Action Coming Soon

- Howard Schmidt predicts a bill this year
- Senate Commerce Bill
- Senate HLS Bill
- House Process different – Congressman Thornberry looking at an incremental approach
- Conference Committee will be key

What (we think) is in the bill

- Establish private sector responsibility for critical infrastructure protection
- Who is covered ? Unclear on what's critical.
- Govt. Role oversight and assure compliance (not fund)
- Legislatively establish the "cyber czar"
- Create mandatory technical standards for "the most critical infrastructure"
- Require bi-annual cyber security audits w/heavy civil fines for non-compliance

Legislative Intent: Senate Consolidated Draft

Summary:

HSGAC-Commerce Staff Draft Cybersecurity Bill

- The bill creates a dynamic partnership between the government and private sector in which the private sector is responsible for enhancing security of the Nation's most critical systems while the government ensures effective oversight and compliance.

ISA Position

- Recognize and deal with 21st century economics
- Can't go back to the future
- Can't regulate your way to growth
- US Govt. needs to partner with industry and provide incentives for innovation, competitiveness and security
- Maintain proper industry and govt. roles
- Detailed industry proposal released 3/7/11

Larry Clinton
President & CEO
Internet Security Alliance
lclinton@isalliance.org
703-907-7028
202-236-0001

www.isalliance.org