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

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**

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

What is our goal?

- Reliability?
- Resilliance?
- Compliance?
- Security?

Why is the Internet Vulnerable?

- It was built that way
- Protocols remain the same and are being adapted
- Use is up dramatically
- New devices make access greater
- We don't pay for security
- Incentives Incentives Incentives
- Its not bad technology, its technology under attack

ISAlliance
Mission Statement

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

The cyber security economic equation

- All the economic incentives favor the attackers
- Attacks are cheap, easy, profitable and chances of getting caught are small
- Defense 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
- DHS has it wrong---efficiency and security are negatively related

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

State of cyber security in utilities (PWC 2011)

- Exec are confident in info security BP
- They have effective plans in place & executing it
- HOWEVER:
- Event frequency is up,
- More sophisticated attacks are occuring
- Operating expenditures crucial to early detection are more likley to be deferred than at any time since 2008

State of cyber security in utilities (PWC 2011)

- 75% of Execs are either very (32%) or somewhat confident that their info security is effective
- 25% are not even somewhat confident
- Awareness of breaches up (80% knowledgeable)
- “Insider” attacks up (partner/suppliers up 67%)
- The confidence rating while high, is actually down 13% since 2006 (84% to 75%)

State of cyber security in utilities (PWC 2011)

- For the third year in a row security spending deferments and cutbacks are high
- Deferred security initiatives 43% in 2009; 48% in 2010; and 48% in 2011
- Reduced funding for security initatives 38% in 2009, 43% in 2010 and 46% in 2011
- 48% predict security spending will increase in the next 12 months (down from 54% who predicted an increase last year)

Cloud Computing is Growing

- 44% of utilities report that their orgianzzations use cloud computing,
- 40% say cloud computing has improved their security
- 62% of all IT professionals say they have “little or no confidence” of the security of the cloud---including 48% who have already placed their data in the cloud
- Difficult to enforce provider security policies

Advanced Persistent Threat—What is it?

- Well funded
- Well organized---state supported
- Highly sophisticated---NOT “hackers”
- Thousands of custom vesions of malware
- Esclate sophistication to respond to defenses
- Maintain their presence and “call-home”
- They target vulnerable people more than vulnerable systems

INTERNET SECURITY ALLIANCE

APT

- “The most revealing difference is that when you combat the APT, you prevention efforts will eventually fail. APT successfully compromises any target it desires”----M-trend Reports
- 18% of APT attacks are against the energy sector
- 5% APT attacks vs the chemical sector
- 49% of utilities say APT is driving their security spending

Utilities Response to APT

- "Utilities are countering the APT principally through virus protection (51%) and either intrusion detection/prevention solutions(27%)
- "Conventional information security defenses don't work vs APT. The attackers successfully evade all anti-virus network intrusion and other best practices, remaining inside the targets network while the target believes they have been eradicated."---M-Trend Reports 2011

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

www.isalliance.org