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

ISA Board of Directors

Ty Sagalow, Esq. Chair
President, Innovation Division, Zurich
Tim McKnight Second V Chair,
CSO**,** Northrop Grumman

J. Michael Hickey, 1st Vice Chair
VP Government Affairs, Verizon
Marc-Anthony Signorino, Treasurer
National Association of Manufacturers

- Ken Silva, Immediate Past Chair, CSO VeriSign
- Lt. Gen. Charlie Croom (Ret.) VP Cyber Security, Lockheed Martin
- Jeff Brown, CISO/Director IT Infrastructure, Raytheon
- Eric Guerrino, SVP/CIO, bank of New York/Mellon Financial
- Pradeep Khosla, Dean Carnegie Mellon School of Computer Sciences
- Joe Buonomo, President, DCR
- Bruno Mahlmann, VP Cyber Security, Dell
- Linda Meeks, VP CISO Boeing Corporation
- Justin Somaini, CISO Symantec

INTERNET SECURITY ALLIANCE

ISAlliance Mission Statement

ISA seeks to integrate advancements in technology with pragmatic business needs and enlightened 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
- We have been focused on the HOW cyber attacks we need to focus on the WHY ($)
- Cyber security is an economic/strategic issue as much operational/technical one

Cyber Security Economics are Skewed

- Responsibility, costs, harms and incentives are misaligned
- Individual and Corporate Financial loss
- National Defense
- Core investment is undermined by edge insecurity
- Enterprises are not structured to properly analyze cyber risk (ANSI-ISA study)

What we do know 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
- Why am I not in this business?

Bad News and Good News

- Bad: The situation is getting worse
- Good: We know how to stop/mitigate 80/90% of cyber attacks
- Bad: Although attacks are up, Investment is down in 50-66% of American firms (PWC/CSIS/Gartner)

Regulation is not the answer

- Compliance (not security) already eats up much of the “security” budget
- Specific Regs can’t keep up with attacks
- Vague regs show no effect
- Regs increase costs uniquly for American companies
- Regs can be counter productive ‘celinings” g(Campaign Finance)

ISA Social Contract Model

- Model on Electric/Telephone “social contract” (November 2008)
- Cyber Space Policy Review (May 2009)
- Social Contract 2.0 (January 2010)

INTERNET SECURITY ALLIANCE

Implementing Obama's Cyber Policy via a Social Contract Model

- Developing a market for standards, practices through market incentives
- Creating an Actionable model for information sharing
- Digital-legal realignment
- Securing the Global IT Supply chain
- Corporate Cyber Financial Risk Management

Incentive based model for cyber security

- Rely on status quo methods to create cyber security standards and practices
- Test for effectivness (e.g. FDA)
- Create tiered levels based on risk profile
- Apply market incentives to vol adoption
- Embraced by CSPR (tax/ liabibility/ procurement/insurance) & legislation

INTERNET SECURITY ALLIANCE

Social Contract: Info Sharing

- We need to be sure information being shared can be put into action…We need to get the roadblocks out of the way
- Most companies w/limited budgets are locked into reactive defensive posture allowing for little more than signature based perimeter monitoring and if detected malware eradication.

INTERNET SECURITY ALLIANCE

Roach Motel: Bugs Get In Not Out

- No way to stop determined intruders
- Stop them from getting back out (w/data) by disrupting attackers command and control back out of our networks
- Identify web sites and IP addresses used to communicate w/malicious code
- Cut down on the “dwell time” in the network
- Don’t stop attacks—make them less useful

INTERNET SECURITY ALLIANCE

New Model (based on AV model)

- Focus not on sharing attack info
- Focus IS ON disseminating info on attacker C2 URLs & IP address & automatically block OUTBOUND TRAFFIC to them
- Threat Reporters (rept malicious C2 channels)
- National Center (clearing house)
- Firewall Vendors (push info into field of devices like AV vendors do now)

The ISA Supply Chain Strategy/Framework

- Solve the supply chain problem in a way that ALSO produces other security benefits thus justifying the increased expenditure
- Businesses are not suffering greatly from supply chain attacks, but are suffering from other attacks
- Key is to make the entire supply chain secure, i.e. supply chain must be part of a comprehensive framework

INTERNET SECURITY ALLIANCE

Framework: Legal Support Needed

1. Rigorous contracts delineating security measures
2. Locally responsible corporations w/long term interest in complying
3. Local ways of motivating workers and executives
4. Adequate provision for verifying implementation of security
5. Local law enforcement of agreements at all levels

ISA Unified Communications Legal Compliance Analysis

(June 2009)

1. Descibes available Unified Communications (UC) Technologies

2. Describes Security Risks of Deployment

3. Inventory of Laws to be considered pre deployment

4. Analysis if ECPA creates a legal barrier to deployment

5 Toolkit for lawyers and clients to assist in avoiding exposure from deployment

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