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

INTERNET SECURITY ALLIANCE

Founders

ISA Board of Directors

Ken Silva, Chairman
CSO Verisgn
Ty Sagalow, Esq. 1st Vice Chair
President Product Development, AIG

J. Michael Hickey, 2nd Vice Chair
VP Government Affairs, Verizon
Dr. M. Sagar Vidyasagar, Treasurer
Exec VP, Tata Consulting Services

- Angie Carfrae, VP Risk Management, Ceridian Corporation
- Tim McKnight, CSO, Northrop Grumman
- Jeff Brown, CISO/Director IT Infrastructure, Raytheon
- Paul Smocer, SVP/CIO, Mellon Financial
- Matt Broda, Chief Strategic Security, Nortel
- Marc-Anthony Signorino, Director Technology Policy, National Association of Manufacturers
- Pradeep Khosla, Dean Carnegie Mellon School of Computer Sciences
- Matt Flanagen, President, Electronic Industries Alliance

INTERNET SECURITY ALLIANCE

Business Services

- Integrating Information Security into the Business Plan (NASDAQ Conference)
- ISAlliance Integrated Security Services Program
  - E-Discovery
  - Outsourcing Risk Management
  - Security Breach Notification
  - Security Incident Handling
  - Auditing
- High Profile Speaking and Article Placements
- Preventing and Detecting Insider Threats
- Best Practices Development
  - Senior Managers Guide to Cyber Security
  - Small Businesses Guide to Cyber Security
  - Home Users & Mobile Executive Guide
- Cyber Insurance Discount Program for Best Practice Compliance (up to 15%)
- Exclusive Annual Privacy Policy Trends Report
- Contracting for Information Security, Model Commercial Agreements Guides
- IT Risk Management Quarterly Work Group

Technical Services

- Weekly Webinars from Carnegie Mellon University on Emerging Info Security issues
- Continuing Education Credit Program in Information Security
- ISAlliance/ANSI Model Terms for Certified ISMS featuring ISO/IEC 27001
- ISAlliance/ANSI Model Commercial Agreements featuring ISO/IEC 17799
- ISAlliance/ISSA Guide to Model Terms for Commercial Agreements
- SQUARE Methodology and Tool
- Online Assessment Tools and Insurance Discounts
- Exclusive Annual Software Assurance Report
- Participation in Critical Infrastructure Protection Planning with U.S. DHS
- Placement of Membership Articles in Professional Journals
  - Fixing Cyber Security Problems
- Daily Threat and Vulnerability Briefings from US-CERT

Legal & Policy Services

- Comprehensive Solutions for E-Discovery
- Interaction with Senior Policy Makers
  - Congress
  - Department of Homeland Security
  - US Department of Commerce Economic Security Working Group
- National Infrastructure Protection Plan
  - IT Sector Coordinating Council
- Member Speaking & Writing Opportunities
  - Cutter IT Journal
- Market Incentives for Cyber Security
  - Market Incentives White Paper
- Congressional Staff Briefings
  - Defense Issues
  - IT & Telecommunications Issues
  - Insider Threats
  - International Issues
- Exclusive Annual Privacy Policy Trends Report
- Privacy Quarterly Work Group

Study Background

- Companies approached former ISA President Dave McCurdy requesting help in addressing supply chain management issues
- Problem has technical components
- Problem has legal components
- Problem has political components
- All need to be addressed
- Need a practical, political, effective solution

Globalization: Pro and Con

- Military, power systems, communications, our economy are dependent on modern information systems---thus they are targets for attack
- Cyber attacks can be perpetrated from software or hardware
- How do we assure the security of critical systems produced off shore?

Globalization Pro and Con

- The IT Supply chain is now inherently globalized
- Operating in a US only fashion would harm our economy
- Harm our security
- Create backlash exacerbating the problem
- We must find a 21st century solution

INTERNET SECURITY ALLIANCE

Research Questions

1. Review current threats/impacts w/ recommendations for mitigation including policy, technology, business R&D
2. Define the threat, how significant is it?
3. What are the best methods being practiced by industry and govt. to resolve it
4. What are the recommended short and long term solutions?

I. CMU Study

1. Carnegie Mellon University would be commissioned to conduct a field study
2. 3 Open conferences
3. Survey data
4. Access to personal interviews
5. Write a Report including recommendations addressing the research questions

II. Experts panel

1. JoAnne Isham
2. Lt. Gen. Harry Rouge
3. Alan Wade
4. John Osterholtz
5. John Nagengast
6. Dr. Leslie Lewis

Industry Analysis

- After CMU study (due Jan 08)
- After Experts Panel analysis (expected 3/08)
- ISA Board and sponsoring organizations will review and make recommendations as to how business can best assist in addressing this issue (expected April/May 08)

Yesterday's Program

- End of the first stage of the three stage effort
- First was an industry/academic conference at CMU in October focused on problem definition
- Second a workshop sponsored by Intel NSF
- Today integrate govt. with industry

The Economics of IT Supply Chain Attacks (Scott Borg)

- Look at Value

- We know we can't defend everything all the time.

- Who might attack?
- What do they want?
- What are their costs and benefits?

Economics of IT Supply Chain Attacks

- Lots of different attackers, but not one amorphous attacker

- Criminals have different motives than angry employees and nation states have different resources than rogue companies)

- Carefully think it through to a practical strategy

What Can you Do?

- Interrupt Operations
- Corrupt Operations
- Discredit Operations
- Remove control of Operations

Motives

(Financial Gain)

- Increase your value by damaging a competitor
- Divert Value (stealing)
- Manipulate Value (financial instrument
- Blackmail via credible attack

INTERNET SECURITY ALLIANCE

Motives

(not financial)

- Advertise
- Stop an Activity
- Attack to reduce the ability to counter attack

Why Use a IT supply Chain Attack?

- "We look at all the different attacks and ways to gain and its striking how few cases an attacker would even think about this attack, except…"
- Most likely is #7 reduce the ability to counter attack
- Get into the supply chain and make all the big weapons equipment unreliable and dysfunctional

INTERNET SECURITY ALLIANCE

What to do?

- Is there any remedy short of controlling the designs and overseeing every step?
- Its about figuring out the supply chain and what you most need to protect/verify and look at and do that
- Manage risk: Create a secure system even with some insecure parts

Today's Program

1. Brief review of economic analysis
2. 2. Dr. Hoe will review the technical issues discussed in the first two workshops
3. Break
4. Industry panel focused on technical/operational issues IBM and Cisco, also Nortel and Savant
5. Gov Tech operational panel NIST and DHS

Today's Program

6. Lunch speaker Tony Sagar NSF
7. Industry panel on legal and policy perspectives (Verizon, Once labs also Lenovo & Infineon)
8. Govt. Panel on legal and policy issues (Andy Purdy former DHS, two Toms FBI and DOE)

Break out sessions built around Research Questions

(please sign up at lunch)

9. Reports back to Plenary

What you can do

- Participate in the discussions
- Participate in the study/interviews
- Participate in the full project