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

ISA Board of Directors

- **Ty Sagalow, Board Chair; President Innovation Division, Zurich North America**
- **Mike Hickey, Board Vise Chair, VP Government Affairs and National Security, Verizon Corp.**
- **Tim McKnight, VP & CISO, Northrop Grumman**
- **Jeff Brown, CISO Information Security, Raytheon**
- **General Charlie Croom (Ret.), VP Cyber Security Solutions, Lockheed Martin**
- **Eric Guerrino, CIO, Bank of New York Mellon**
- **Pradeep Khosla, Dean, School of Computer Sciences, Carnegie Mellon U**
- **Lawrence Dobranski, Security Manager, Nortel**
- **Mark Anthony Signorino, Chief Technology, Nat. Assoc Manufacturers**
- **Joe Buonomo, President, Direct Computer Resources Inc.**

INTERNET SECURITY ALLIANCE

Our Partners

STAYSAFEONLINE.org
National Cyber Security Alliance

US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

UNITED STATES DEPARTMENT OF THE TREASURY

FCC Federal Communications Commission

BSI

ANSI
American National Standards Institute

ISSA
Information Systems Security Association
The Global Voice of Information Security

NFIB
The Voice of Small Business®

IT SCC
INFORMATION TECHNOLOGY SECTOR COORDINATING COUNCIL

Council on Competitiveness

AMERICAN BANKERS ASSOCIATION

ISA Mission

Integrate technology with economically practical business considerations and public policy to create a sustainable system of cyber security

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

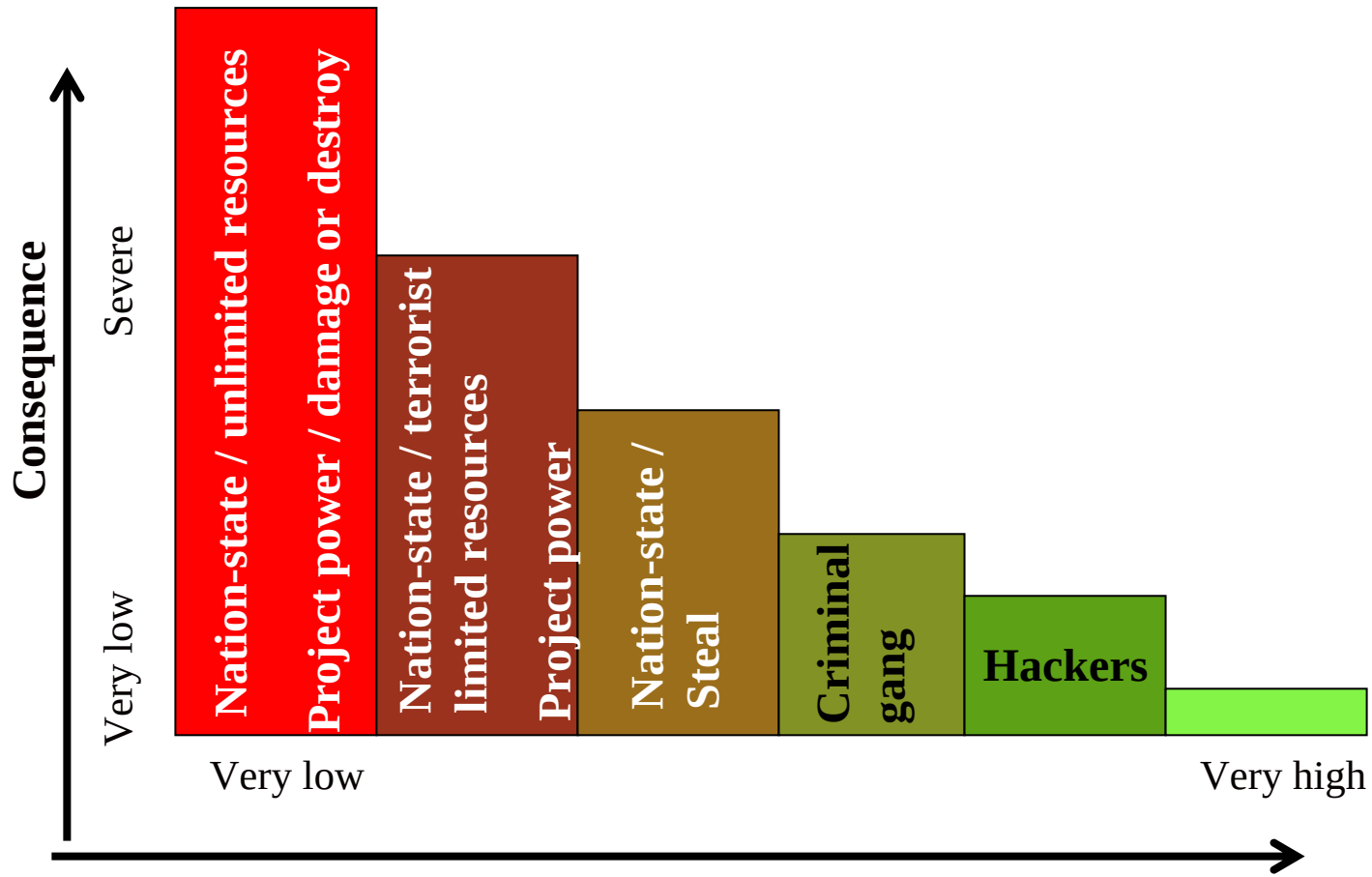
Technical Services

- 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

National Risk Continuum



2009 ISA Priority Projects

1. Create a Cyber Security Social Contract between business and government to provide market incentives for improved security
2. Develop Best Practices for financial risk management of cyber incidents
3. Create a framework for managing conflicting legal structures and unified communications tech.
4. Develop standards to secure the VOIP platform

ISA Supply Chain Project

- 18 months long (start fall 07)
- Focus on firmware
- Carnegie Mellon University and Center for Cyber Consequences Unit
- 3 conferences
- 100 Gov., Industry and Academic participants
- Results are strategy and framework provided to USG for NSC 60-day review of cyber policy

ISA/CMU Study Results

1. Globalization of IT Supply Chain will increase
2. USG reliance on IT will also increase
3. Threat from IT supply chain significant for USG
4. “USG-only” solution impractical
5. Attackers will be fluid and creative so fixed policies will be ineffective long term
6. Need a flexible framework of solutions

Framework: Danger of Malicious Firmware

- Serious danger of infiltrating the supply chain
- Altered circuitry to transfer control over info systems
- A logic bomb could lay dormant then activate at the worst possible moment
- A weapons system could be shut down when needed, or even turned against the owner
- Virtually impossible to detect
- Domestic sole sourcing is

Framework: Economic Issues

- Supply chain attacks are very difficult and expensive
- Almost always cheaper and more effective to use more traditional cyber attacks
- NATION STATES CAN AFFORD AND MIGHT BE WILLING TO INVEST IN SUPPLY CHAIN ATTACKS
- Some criminal conspiracies might also be willing to conduct supply chain attacks
- Malicious firmware is a serious

Types of Supply Chain Attacks & Remedies

1. Interrupt Operation: Maintain alternative sources and continual sharing of production across chain

2. Corrupt Operation (e.g. insert malaria): strict control of environment where key IP is being applied, logical and physical tamper proof seals/tracking containers

3. Discredit the operation (undermine trust or brand value): logging operation and responsibility

4. Loss of information: Versioning as a

Framework: Stages When Attacks May Occur

1. Design Phase
2. Fabrication Phase
3. Assembly Phase
4. Distribution Phase
5. Maintenance Phase

Supply Chain
Remedies for Stages Grid

	REMEDIES			
STAGES				

Framework: Legal Support Needed

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

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