INTERNET
SECURITY
ALLIANCE

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

INTERNET SECURITY ALLIANCE

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

Our Partners

EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES • OFFICE OF MANAGEMENT AND BUDGET

UNITED STATES SENATE

U.S. HOUSE OF REPRESENTATIVES

EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES • OFFICE OF MANAGEMENT AND BUDGET

U.S. DEPARTMENT OF HOMELAND SECURITY

DEPARTMENT OF COMMERCE UNITED STATES OF AMERICA

NATIONAL SECURITY AGENCY UNITED STATES OF AMERICA

CENTRAL INTELLIGENCE AGENCY UNITED STATES OF AMERICA

DEPARTMENT OF JUSTICE FEDERAL BUREAU OF INVESTIGATION

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

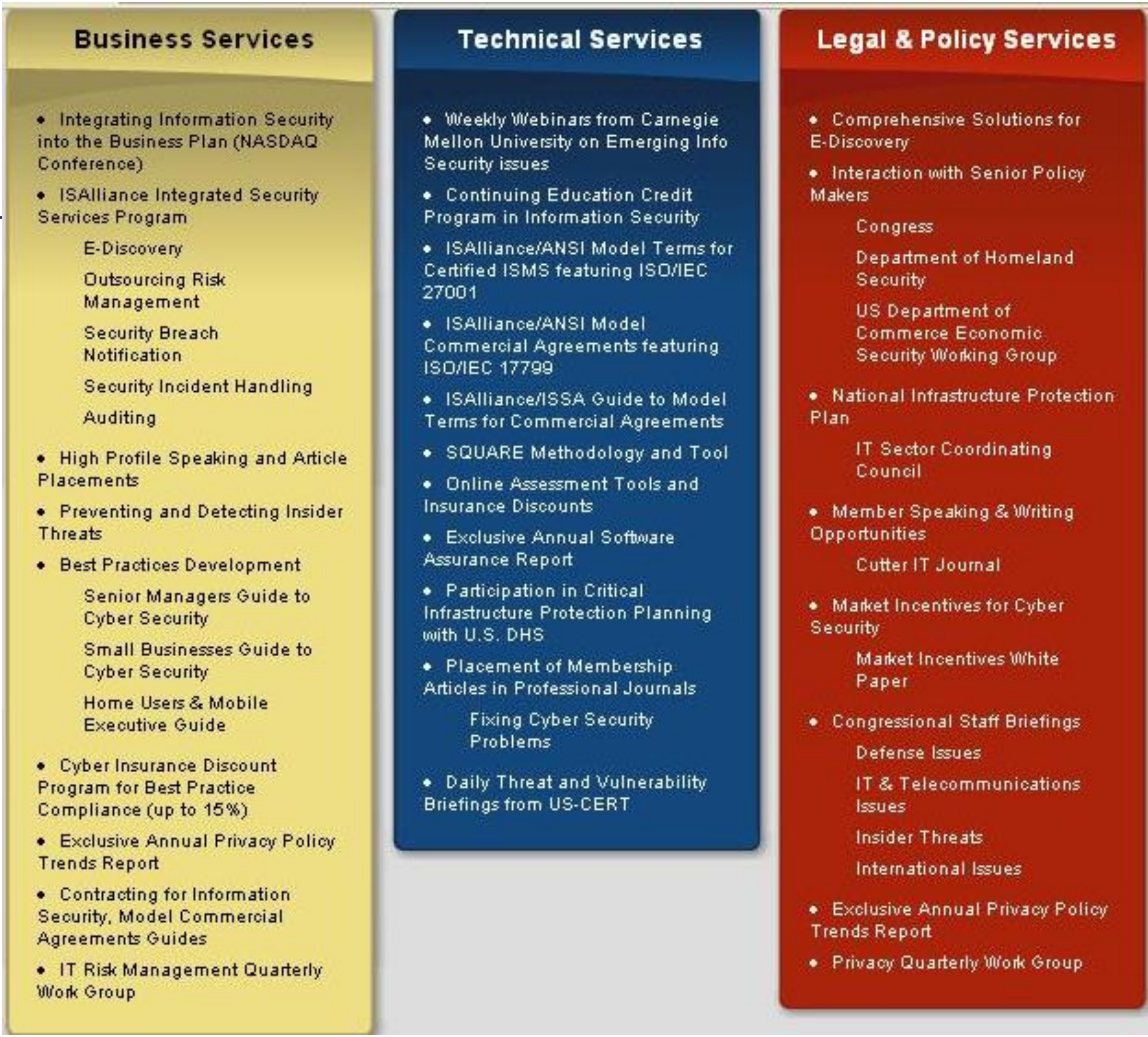
NFIB
The Voice of Small Business®

INFORMATION TECHNOLOGY
IT SCC
SECTOR COORDINATING COUNCIL™

Council on Competitiveness

AMERICAN BANKERS ASSOCIATION

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

Digital Growth? Sure

"Companies have built into their business models the efficiencies of digital technologies such as real time tracking of supply lines, inventory management and on-line commerce. The continued expansion of the digital lifestyle is already built into almost every company's assumptions for growth."

---Stanford University Study, July 2006

Digital Defense? Maybe Not

29% of Senior Executives "acknowledged" that they did not know how many negative security events they had in the past year

50% of Senior Executives said they did not know how much money was lost due to attacks

Source: PricewaterhouseCoopers survey of 7,000 companies 9/06

INTERNET SECURITY ALLIANCE

Digital Defense ------ Not So Much

23% of CTOs did not know if cyber losses were covered by insurance.

34% of CTOs thought cyber losses would be covered by insurance----and were wrong.

“The biggest network vulnerability in American corporations are extra connections added for senior executives without proper security.”

---Source: DHS Chief Economist Scott Borg

Changing Nature of Attacks

Vulnerabilities are on client-side applications word, spreadsheets, printers, etc.

“The future threat landscape around the world will be dictated by the soon-to-be-released Apple iPhone, Internet telephony and Internet video-sharing, and other Web-based innovations” (McAfee 2007)

Today, attackers perpetrate *fraud*, gather *intelligence*, or conduct *blackmail*

Applying the SAFETY Act

- SAFETY Act Passed following 911 to encourage the development of anti-terrorism technologies
- Insurance benefits, liability protection, marketing benefits
- Initially difficult for Corporations to manage and focused on high value physical threats
- New focus on cyber including an expanded concept of threat and terrorism
- ISA providing aid to companies to get SAFETY

INTERNET SECURITY ALLIANCE

Securing the Global IT Supply Chain

- IT supply chain is inherently global
- This immutable reality brings new risks
- If not addressed Congress will do it for us, probably through protectionism
- Bad for everyone
- ISA/CMU/industry 3-phase program to analyze the situation and create a solution that takes into account market, business and policy reality

INTERNET SECURITY ALLIANCE

Securing the VOIP Platform

- VOIP is the paradigm case for corporate economics overcoming security concerns
- Platform itself not a profitable as products sold to use it
- ISA/NIST program to use SCAP (Security Content Automation Protocol) and National Vulnerability Database to create a free customizable framework -- better market security products.
- Better security and better markets

Develop a Framework for Corporate Cyber Risk

- Grows out of 911 legislation passed in 2007
- Bring cyber risk analysis to all relevant areas of corporate culture (not just IT)
- Develop a tool allowing for more standardized internal analysis and action
- Multi-dimensional approach Including legal/ regulatory/ compliance/operations/insurance/ governance external communications

INTERNET SECURITY ALLIANCE

Legal/Regulatory Issues

- Have cyber liabilities been analyzed?
- What regulations apply to lines of business?
- Exposed to class action/shareholder suits?
- Is org protected from business interruptions?
- Org protected from fed/state govt. investigations?
- What jurisdictions does date move through?
- What is in our contracts?
- What does our privacy policy say?

Compliance/Regulatory

- Have an inventory of what regs apply to us?
- Know what reg data is and where its located?
- Valid reasons for keeping this data?
- What have we done to protect the data?
- Incident response program/notification program?
- What is impact of possible data loss?
- Procedures in place for tracking compliance?
- How are we tracking vendors procedures?

INTERNET SECURITY ALLIANCE

External Rel & Comm.

- Analyzed impact of events on reputation/ stakeholders/customers etc?
- Plan for communicating with stakeholders?
- Identified resources/budget needed for plan?
- Clear roles and responsibilities for comm?
- Thought through segmenting messages for different stakeholders?
- Legal requirements for notification? Tested it?

Risk transfer

- What is exposure (brand/confidence/physical loss?—how do we measure?
- Are you already covered? D&O?
- Do we need to bring in expertise? Who?
- Is insurance available?
- What is the ROI for insurance and other risk transfer approaches?

INTERNET
SECURITY
ALLIANCE

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