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

Board of Directors

Ty Sagalow, Esq. Chair President, Innovation Division, Zurich
J. Michael Hickey, 1st Vice Chair VP Government Affairs, Verizon
Tim McKnight Second V Chair CSO**,** Northrop Grumman

- **Joe Buonomo**, President, DCR
- **Jeff Brown**, CISO/Director IT Infrastructure, Raytheon
- **Lt. Gen. Charlie Croom (Ret.)** VP Cyber Security, Lockheed Martin
- **Paul Davis**, CTO, NJVC
- **Eric Guerrino,** SVP/CIO, Bank of New York/Mellon Financial
- **Pradeep Khosla**, Dean Carnegie Mellon School of Computer Sciences
- **Bruno Mahlmann**, VP Cyber Security, Dell
- **Gary McAlum,** CSO, USAA
- **Kevin Meehan**, VP & CISO, Boeing
- **Andy Purdy**, Chief Cybersecurity Strategist, CSC
- **Ken Silva**, CSO, VeriSign
- **Justin Somaini**, CISO Symantec

ISAlliance Mission Statement

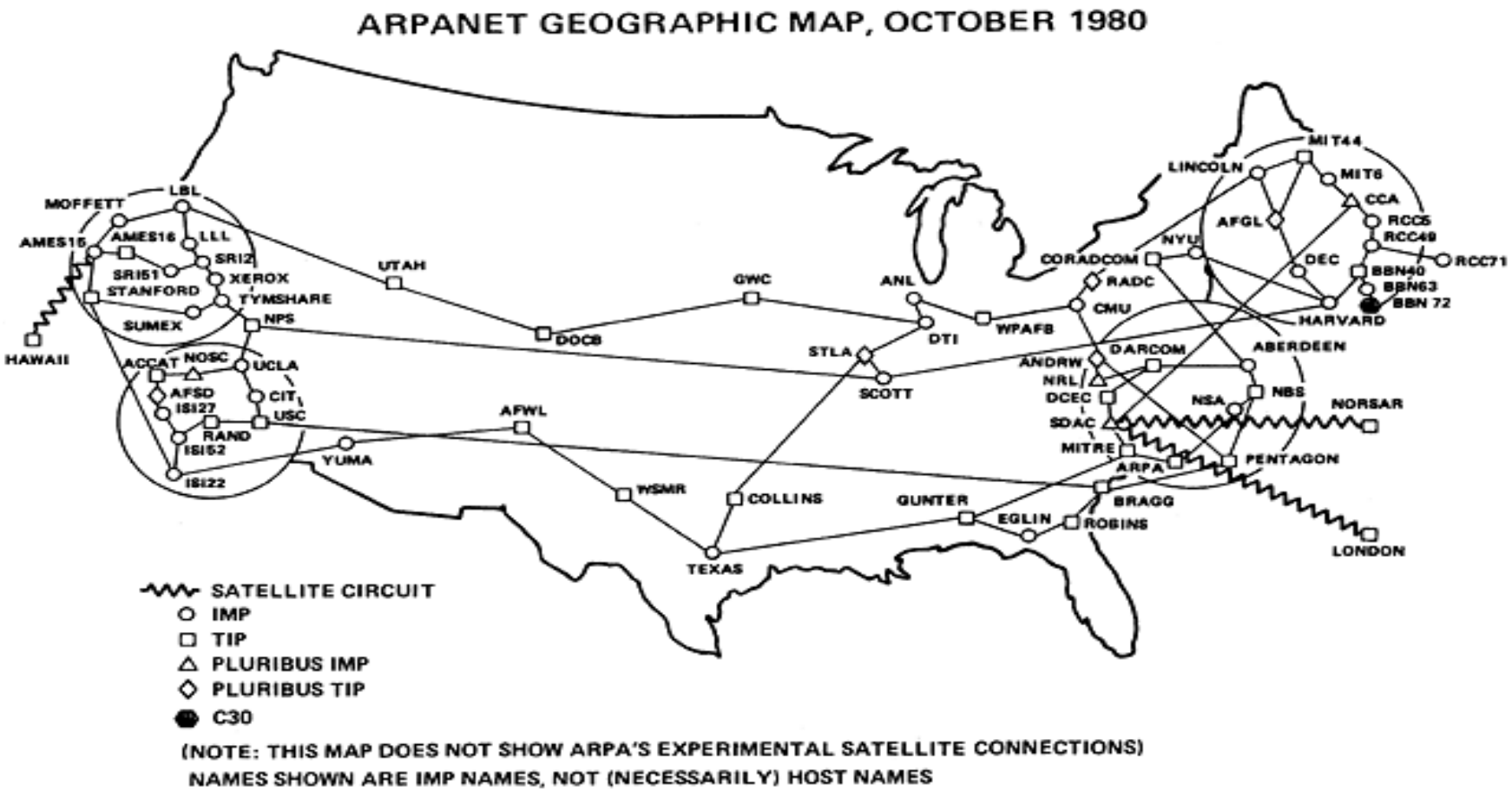
ISA seeks to integrate advancements in technology with pragmatic business needs and enlightened public policy to create a sustainable system of cyber security.

ISA Priority Programs

- Security standards for VOIP-Smart Phones CCP
- Securing the Global IT Supply Chain
- New Model for information sharing
- Navigating Compliance with advanced technology and multiple jurisdictions
- The Cyber Security Social Contract (Partnership model for industry and govt. based on market principles
- Corporate financial risk management of cyber security

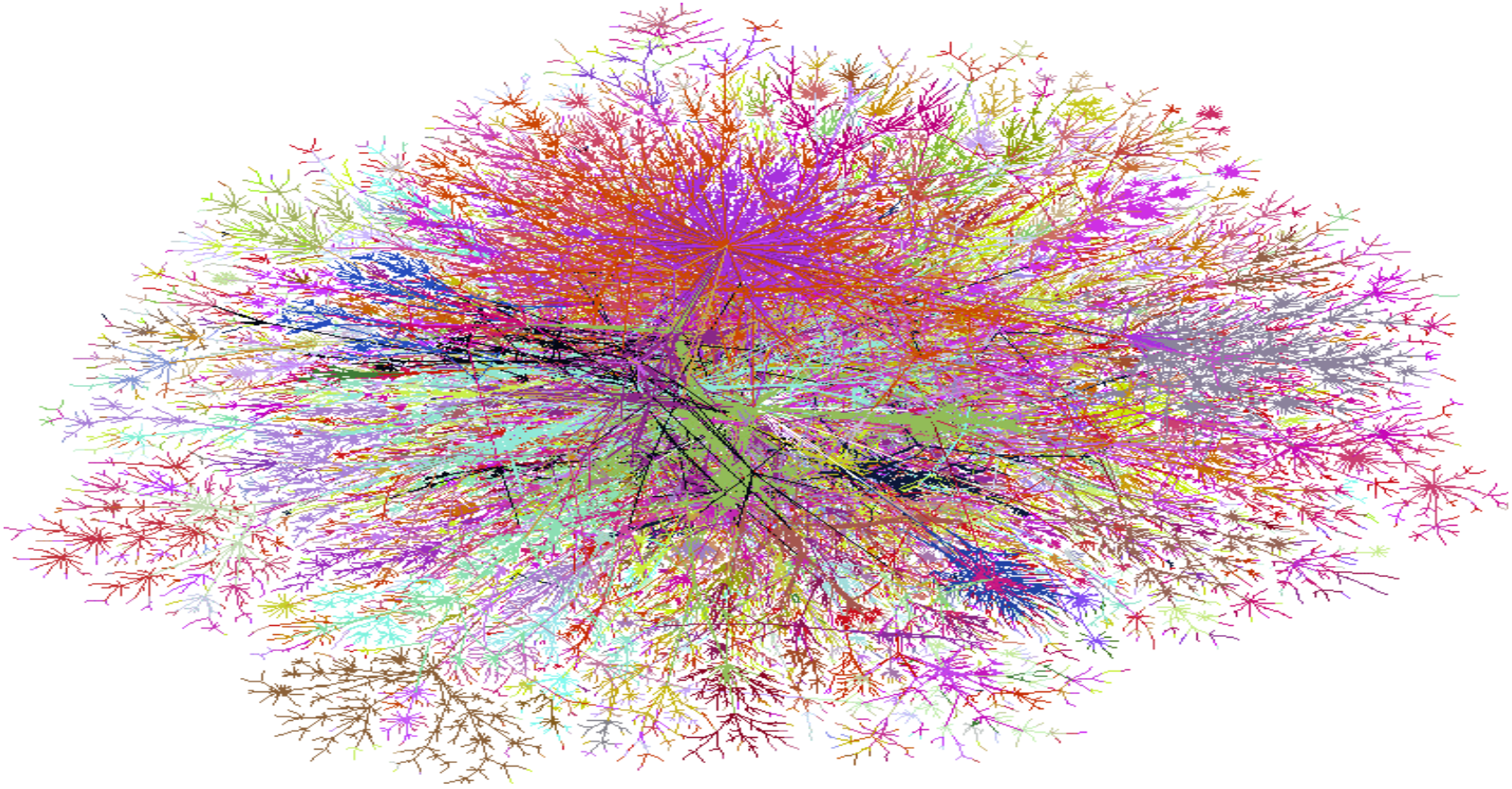
INTERNET SECURITY ALLIANCE

The Past



INTERNET SECURITY ALLIANCE

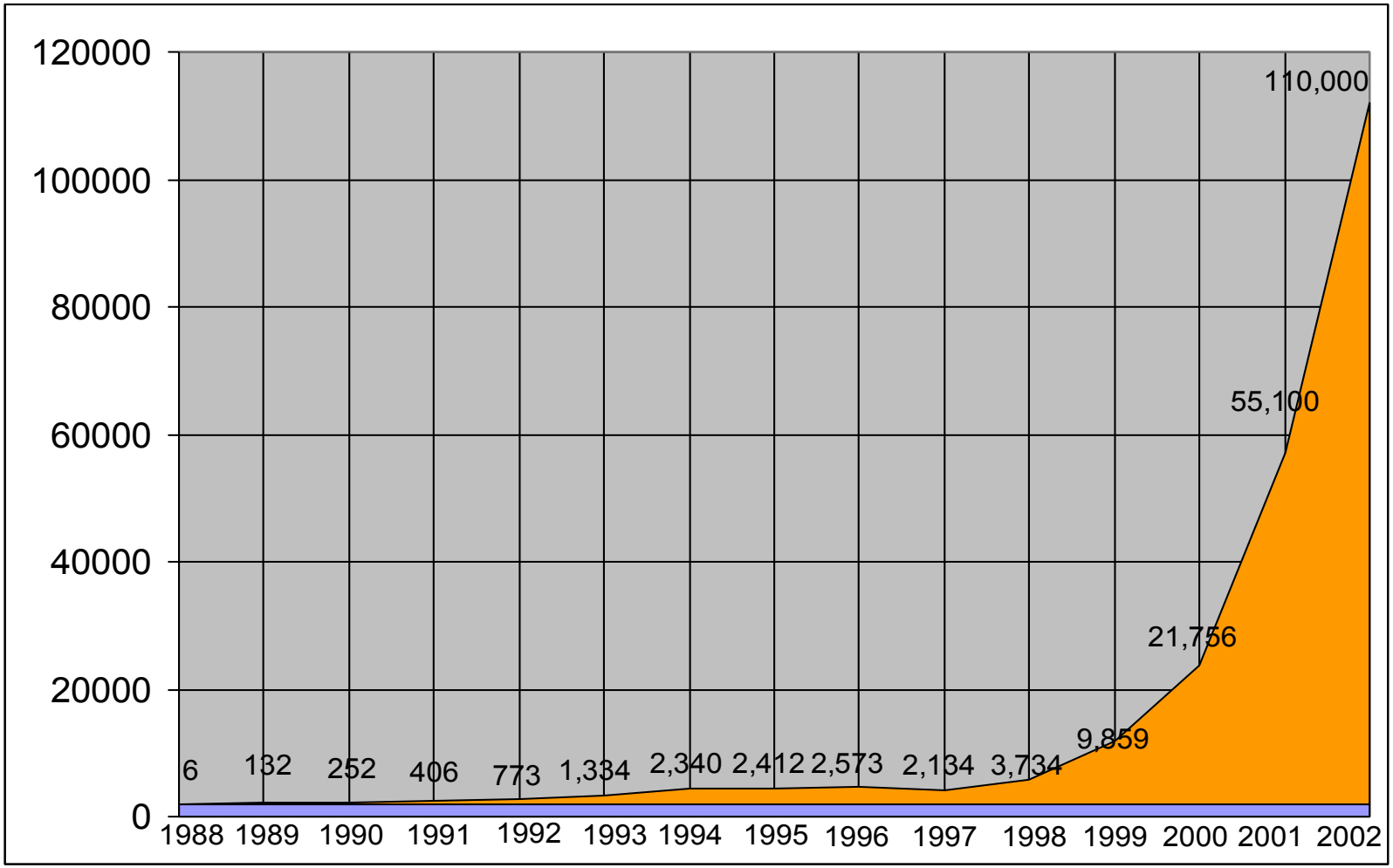
The Present



Source: http://cm.bell-labs.com/who/ches/map/gallery/index.html

INTERNET SECURITY ALLIANCE

Growth in Incidents Reported to the CERT/CC



INTERNET SECURITY ALLIANCE

History of Cyber Security

- The computer Revolution
- The desktop Revolution
- The broadband/digital revolution
- Y2K
- Attacks for grins and giggles
- The perimeter defense/resiliency model
- The information sharing approach

INTERNET SECURITY ALLIANCE

Faces of Attackers… Then

Joseph McElroy

Hacked US Dept of Energy

Jeffrey Lee Parson

Blaster-B Copycat

Chen-Ing Hau

CIH Virus

INTERNET SECURITY ALLIANCE

Faces of Attackers… Now

Jay Echouafni

Competitive DDoS

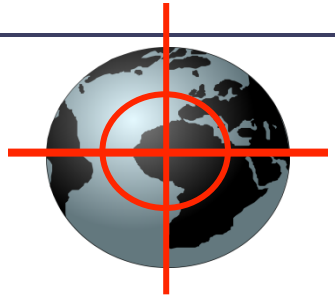
Jeremy Jaynes

$24M SPAM KING

Andrew Schwarmkoff

Russian Mob Phisher

The Threat Landscape is Changing



Early Attacks

Defense: Reactive AV signatures

Recovery: Scan & remove

Type: Virus, worm, spyware

New Era Attacks

Multi-layer pre-emptive and behavioral systems

System wide, sometimes impossible without re-image of system

Targeted malware, root kits, spear phishing, ransom ware, denial of service, back door taps, trojans, IW

INTERNET SECURITY ALLIANCE

The Internet Now

- Vulnerabilities are on client-side applications word, spreadsheets, printers, etc.
- Today, attackers perpetrate *fraud*, gather *intelligence*, or conduct *blackmail*
- *The number of new threats to the Internet jumped 500% between 2006 and 2007 and doubled again between 2007 and 2008---1000% increase---- Symantec*

INTERNET SECURITY ALLIANCE

Characteristics of the New Attackers

- Shift to profit motive
- Zero day exploits
- Increased investment and innovation in malcode
- Increased use of stealth techniques

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

How Series a problem do we have?

- Vulnerabilities and attacks increasing at a pace too difficult to count
- Loss estimates are between billions and a trillion
- The National Intelligence Estimate
- The APT
- Suxtnet
- We don't know what we don't know---it could be worse…

INTERNET SECURITY ALLIANCE

Advanced Persistent Threat (APT)

"We have seen a dramatic change in info security incidents. Superbly capable teams of attackers have successfully expanded their attacks…These intrusions are well funded and organized. They are not hackers. Their motivations and techniques are different. *They are professionals and their success rate is impressive. They successfully evade antivirus & network intrusion and remain inside the targets network while the target believes they have been eradicated. Their motive is to steal data & establish a way to come back later and steal more.*"

INTERNET SECURITY ALLIANCE

The Insider Threat

This year marks the first time "employees" beat out "hackers" as the most likely source of a security incident. Executives in the security field, with the most visibility into incidents, were even more likely to name employees as the source.

----PricewaterhouseCoopers 2010 Global Information Security Survey

INTERNET SECURITY ALLIANCE

Cyber Security and the Economy

The state of Internet security is eroding quickly. Trust in online transactions is evaporating, and it will require strong security leadership for that trust to be restored. For the Internet to remain the juggernaut of commerce and productivity it has become will require more, not less, input from security.

----PWC Global Cyber Security Survey

CSIS Global Info Security Study 2010

- Critical infrastructure operators report their IT networks are under repeated cyber attacks by high level adversaries (including foreign govts) The impact is severe the costs high and borne widely.
- Oil and Gas had the highest degree of penetration at 71% (compared with 54% overall) with potential for large scale power outages or man made environmental disasters
- Costs from attacks up to $6 million a day w/ considerable variation in expectation as to who will bear the costs.

INTERNET SECURITY ALLIANCE

Cyber Economics is not well understood

- Costs for bad behavior are not transparent and always born by the bad actor
- Attacks on the edge of the network (w/out incentive to secure) are used to steal from the core of the network (where security investment is undermined)
- Industry is on the front lines to defend vs. cyber attacks and is expected to pay for this government function
- Industry and Govt. economics are very different

INTERNET SECURITY ALLIANCE

CURRENT ECONOMIC INCENTIVES FAVOR ATTACKERS

- Attacks are cheap and easy
- Vulnerabilities are almost infinite
- Profits from attacks are enormous
  ($ 1 TRILLION in 08)
- Defense is costly (Usually no ROI)
- Defense is often futile
- Costs of Attacks are distributed

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*

INTERNET SECURITY ALLIANCE

Cost Issues: CSIS 2010

Overall, cost was most frequently cited as "the biggest obstacle to ensuring the security of critical networks. p14

Making the business case for cybersecurity remains a major challenge, because management often does not understand either the scale of the threat or the requirements for a solutions. p14

The number one barrier is the security folks who haven't been able to communicate the urgency well enough and they haven't actually been able to persuade the decision makers of the reality of the threat. p14

Making the business case for security could be a challenge – no one wants to pay their insurance bill until the building burns down. p15

INTERNET SECURITY ALLIANCE

Cost Issues PWC 2011

- "Executives worldwide have been reluctant to release funding to support Info security.
- "As spending constraint continues "block and tackle" security capabilities that took decades to build up are degrading creating new levels of risk'
- "Increased risk elevates the importance of security & ongoing cost reduction makes adequate security difficult to achieve."
- 47% reported decreasing info security spending in 2010, same as in 2009"

INTERNET SECURITY ALLIANCE

We are not cyber structured

- In 85% of companies the CFO is not directly involved in information security
- 2/3 of companies don't have a risk plan
- 83% of companies don't have a cross organizational privacy/security team
- Less than ½ have a formal risk management plan —1/3 of the ones who do don't consider cyber in the plan
- In 2010 50%-66% of companies are deferring or reducing investment in cyber security

The Good News: We know (mostly)what to do!

- PWC/GI Information Study 2006--- best practices 100%
- CIA 2007---90% can be stopped
- Verizon 2008—87% can be stopped
- NSA 2009---80% can be prevented
- Secret Service/Verizon 2010---94% can be stopped or mitigated by adopting inexpensive best practices and standards already existing

Are We doing it? CIOnet

- 84% have analyzed cyber liabilities (very good)
- 82 %have audits (1/5 do not audit)
- 72% training (28% do not train)
- 68% discipline policy (32% do not)
- 80% assess biggest vulnerability at least 1 a year
- 65% update incident response plans 1 a year
- 40% Crisis management & enhanced tech know
- 0 % Monetary incentives

INTERNET SECURITY ALLIANCE

WARNING !!!!!!!!!!!!!!!!!

THIS IS NOT MY DATA

Baseline: How is Europe Doing? (PWC data)

"With confidence, persistence and momentum, Asia lines up on the runway to become the new global leader in information security. With more caution and restraint and without the same promise of growth that Asia expects—North America idles its engines. South America presses the gas pedal and the breaks at the same time, while Europe displays a marked lack of direction and urgency"

----Global Info Security Study 2010

More on How Europe is Doing (PWC data)

Europe now trails other regions in maturity across most security capabilities. Europe continues to suffer poor visibility into security events and as a result may be unaware of the true impact of events on business. And while 68% or European respondents say their organization places a high level of importance on protecting sensitive customer information, the responses from other global regions (Asia 80%, N American 80% and S America (76%) reflect more conviction and urgency.

-----Global Info Security Survey 2010

INTERNET SECURITY ALLIANCE

We need a total risk management approach

The security discipline has so far been skewed toward technology—firewalls, ID management, intrusion detection—instead of risk analysis and proactive intelligence gathering.

PWC Global Cyber Security Survey

We have to shift our focus from considering cybersecurity as a technical-operational issue to a economic-strategic issue

Obama: What We Need to Do

It is not enough for the information technology workforce to understand the importance of cybersecurity; leaders at all levels of government and industry need to be able to make business and investment decisions based on knowledge of risks and potential impacts.

Obama Administration Cyber Space Policy Review
May 30, 2009 page 15

INTERNET SECURITY ALLIANCE

What Role for CIO?

- "There is a significant shift in the ongoing evolution of the CISOs reporting channel away from the CIO in favor of the companies senior business decision makers" (PWC 2011 Global Survey)
- Reporting Relationships of the CISO 2007-2010

To CIO----------	23%	(down 39%)
To CEO ----------	36 %	(up 13%)
To CFO ----------	15%	(up 36%)
To COO----------	15%	(up 67%)

INTERNET SECURITY ALLIANCE

ANSI-ISA Program

- Outlines an enterprise wide process to attack cyber security broadly and economically
- CFO strategies
- HR strategies
- Legal/compliance strategies
- Operations/technology strategies
- Communications strategies
- Risk Management/insurance strategies

INTERNET SECURITY ALLIANCE

What CFO needs to do

- Own the problem
- Appoint an enterprise wide cyber risk team
- Meet regularly
- Develop an enterprise wide cyber risk management plan
- Develop an enterprise wide cyber risk budget
- Implement the plan, analyze it regularly, test and reform based on EW feedback

INTERNET SECURITY ALLIANCE

Human Resources

- Recruitment
- Awareness
- Remote Access
- Compensate for cyber security
- Discipline for bad behavior
- Manage social networking
- Beware of vulnerability especially from IT and former employees

INTERNET SECURITY ALLIANCE

Legal/Compliance Cyber Issues

- What rules/regulations apply to us and partners?
- Exposure to theft of our trade secrets?
- Exposure to shareholder and class action suits?
- Are we prepared for govt. investigations?
- Are we prepared for suits by customers and suppliers?
- Are our contracts up to date and protecting us?

INTERNET SECURITY ALLIANCE

Operations/IT

- What are our biggest vulnerabilities? Re-evaluate?
- What is the maturity of our information classification systems?
- Are we complying with best practices/standards
- How good is our physical security?
- Do we have an incident response plan?
- How long till we are back up?---do we want that?
- Continuity Plan? Vendors/partners/providers plan?

INTERNET SECURITY ALLIANCE

Communications

- Do we have a plan for multiple audiences?
  --general public
  --shareholders
  --government/regulators
  --affected clients
  --employees
  --press

INTERNET SECURITY ALLIANCE

Insurance— Risk Management

- Are we covered?----Are we sure?????????
- What can be covered
- How do we measure cyber losses?
- D and O exposure?
- Who sells cyber insurance & what does it cost?
- How do we evaluate insurance coverage?

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

www.isalliance.org