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

During the Last Minute…

- 45 new viruses
- 200 new malicious web sites
- 180 personal identities stolen
- 5,000 new versions of malware created
- 2 million dollars lost

INTERNET SECURITY ALLIANCE

Presentation Outline

- The evolved cyber threat
- What drives the evolved cyber threat
- Economics and cyber security
- Ineffective corporate strategy
- Ineffective Government Policy
- Promising corporate approaches to the new threats
- Promising Public Policy to deal with cyber

Advanced Persistent Threat—What is it?

- Well funded
- Well organized---state supported
- Highly sophisticated---NOT “hackers”
- Thousands of custom versions of malware
- Escalate sophistication to respond to defenses
- Maintain their presence and “call-home”
- They target vulnerable people more than vulnerable systems

What Makes the APT Different

INTERNET SECURITY ALLIANCE

APT

- “The most revealing difference is that when you combat the APT, your prevention efforts will eventually fail. APT successfully compromises any target it desires.”----M-trend Reports

The APT----Average Persistent Threat

"The most sophisticated, adaptive and persistent class of cyber attacks is no longer a rare event…APT is no longer just a threat to the public sector and the defense establishment …this year significant percentages of respondents across industries agreed that APT drives their organizations security spending." PricewaterhouseCoopers Global Information Security Survey September 2011

Government Report

"Online industrial spying presents a growing threat to US economy and national security…tens of billions of dollars of trade secretes, technology and intellectual property are being siphoned each year from computer systems of US government, corporations and research institutions."

US Office of National Counterintelligence

November 2, 2011

ISAlliance
Mission Statement

ISA seeks to integrate advanced technology with business economics and public policy to create a sustainable system of cyber security.

The Cyber Security Economic Equation

- All the economic incentives favor the attackers
- Attacks are cheap, easy, profitable and chances of getting caught are small
- Defense is a generation behind the attacker, the perimeter to defend is endless, ROI is hard to show
- Until we solve the cyber economics equation we will not have cyber security
- DHS has it wrong---efficiency and security are negatively related

Technology or Economics?

"We find that misplaced incentives are as important as technical design…security failure is caused as least as often by bad incentives as by bad technological design"

Anderson and Moore "The Economics of Information Security"

Misaligned Incentives

"Economists have long known that liability should be assigned to the entity that can manage risk. Yet everywhere we look we see online risk allocated poorly…people who connect their machines to risky places do not bear full consequences of their actions. And developers are not compensated for costly efforts to strengthen their code."

Anderson and Moore "Economics of Information Security"

Efficiency and Security

- Business efficiency demands less secure systems (VOIP/international supply chains/Cloud)
- Profits for advanced tech are not used to advance security
- Regulatory compliance is not correlated with security…may be counter productive

Why China and the APT?

"Countries that grow by 8-13% can only do this by copying. Copying is easy at first—you copy simple factories—but to grow by more than 8% you need serious know how. There are only 2 ways to get this: partnering and theft. China cannot afford to NOT to grow 8% yearly. Partnering won't transfer enough know how to sustain 8%+ so all that's left is theft and almost all the theft is electronic." Scott Borg, US Cyber Consequences Unit

Gov and Industry Economics are Different

- We must have public private partnership
- Gov and industry goals are aligned, not identical
- Lack of Trust impedes partnership
- Economics are different for gov and industry
- Difficult issues with respect to risk management, information sharing, roles and responsibilities

% Who Say APT Drives Their Spending

- 43% Consumer Products
- 45% Financial services
- 49% entertainment and media
- 64% industrial and manufacturing sector
- 49% of utilities

PWC 2001 Global Information Security Survey

Are we thinking of APT all wrong?

- "Companies are countering the APT principally through virus protection (51%) and either intrusion detection/prevention solutions (27%) –PWC 2011
- "Conventional information security defenses don't work vs. APT. The attackers successfully evade all anti-virus network intrusion and other best practices, remaining inside the targets network while the target believes they have been eradicated."---M-Trend Reports 2011

INTERNET SECURITY ALLIANCE

We Are Not Winning

"Only 16% of respondents say their organizations security policies address APT. In addition more than half of all respondents report that their organization does not have the core capabilities directly or indirectly relevant to countering this strategic threat.

Administration Legislative Proposal

- DHS defines “covered critical infrastructure”
- DHS sets regulations for private sector via rulemaking establishing frameworks
- PS corps must submit plans to meet regs
- DHS certifies “evaluators” which companies must hire to review DHS approved cyber plans
- Companies DHS decides are not meeting the regs must face public disclosure (name and shame)

INTERNET SECURITY ALLIANCE

Why It Won't Work

- General "Plans" don't tell us anything (but do increase cost and take away from real security)
- Most most successful attacks are difficult and expensive, to find—often you don't know.
- "Disclosure" requirements penalize good companies
- "Name and shame" provides incentives NOT to invest in the expensive tools we need or even look
- If name and shame worked it incentivizes attacks

Why It Won't Work

As I study these pieces of legislation, the one thing that concerns me is the potential negative implications and unintended consequences of creating more security compliance requirements. Regulation and the consequent compliance requirements could boost costs and misallocate resources without necessarily increasing security due to placing too much emphasis on the wrong things. ----Mark Weatherford US Cyber DHS

Why Admin Legislative Plan wont work

> "It is critical that any legislation avoids diverting resources from accomplishing real security by driving it further down the chief security officer's (CSO's) stack of priorities."

Mark Weatherford "Government Technology magazine July 28, 2011

Weatherford was named Under Secretary for Cyber Security in September 2011

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
- **Valerie Abend** 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
- **Tom Kelly**, VP & CISO, Boeing
- **Andy Purdy**, Chief Cybersecurity Strategist, CSC
- **Rick Howard,** iDefense General Manager, VeriSign
- **Cheri Maguire**, VP Global Cyber Security Symantec

ISA and APT

- Roach Motel Model 2008 (Jeff Brown Raytheon Chair)

- Expanded APT best Practices (Rick Howard, VeriSign, Tom Kelly Boeing and Jeff Brown co-chairs)

Old Model for Info Sharing

- Big Orgs may invest in Roach Motel (traffic & analytical methods) small orgs. never will
- Many entities already rept. C2 channels (AV vend/ CERT/DIB/intelligence etc.)
- Perspectives narrow
- Most orgs don't play in info sharing orgs
- Info often not actionable
- Lack of trust

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 add & 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)

Corp. Due Diligence

- Physical separation between the corporate network, the secret sauce, any Merger & Acquisition (M&A) groups and any contract deals
- Enforce the "Need to Know" rule
- Encrypt everything in transit & at rest e.g. Smartphone.
- Foreign travel. Use throw-away laptops and
- Label all documents and e-mail with the appropriate data classification
- Upgrade to the latest operating systems

Preventing and Identifying Exploitation

- Identify vulnerable software.
- Prevent exploitation by enumerating applications with Microsoft EMET.
- Train and maintain vigilance of employees regarding the sophistication of spoofed and technical social engineering attacks.
- Applying email filters and translation tools for common attack file types like PDF and Office Documents.
- Installing and testing unknown URLs with client honeypots before delivering email and allowing users to visit them.

Outgoing Data and Exfiltration

a. Monitor all points of communication (DNS, HTTP, HTTPS) looking for anomalies
b. Limit access to unknown communication types
c. Utilize a proxy to enforce known communication and prevent all unknown communication types.
d. Monitor netflow data to track volume, destination,
e. Monitor free and paid services like webhosting.

Understand APT Why Are You a Target?

- Collection Requirements typically focus on 3 areas:

a) Economic Development

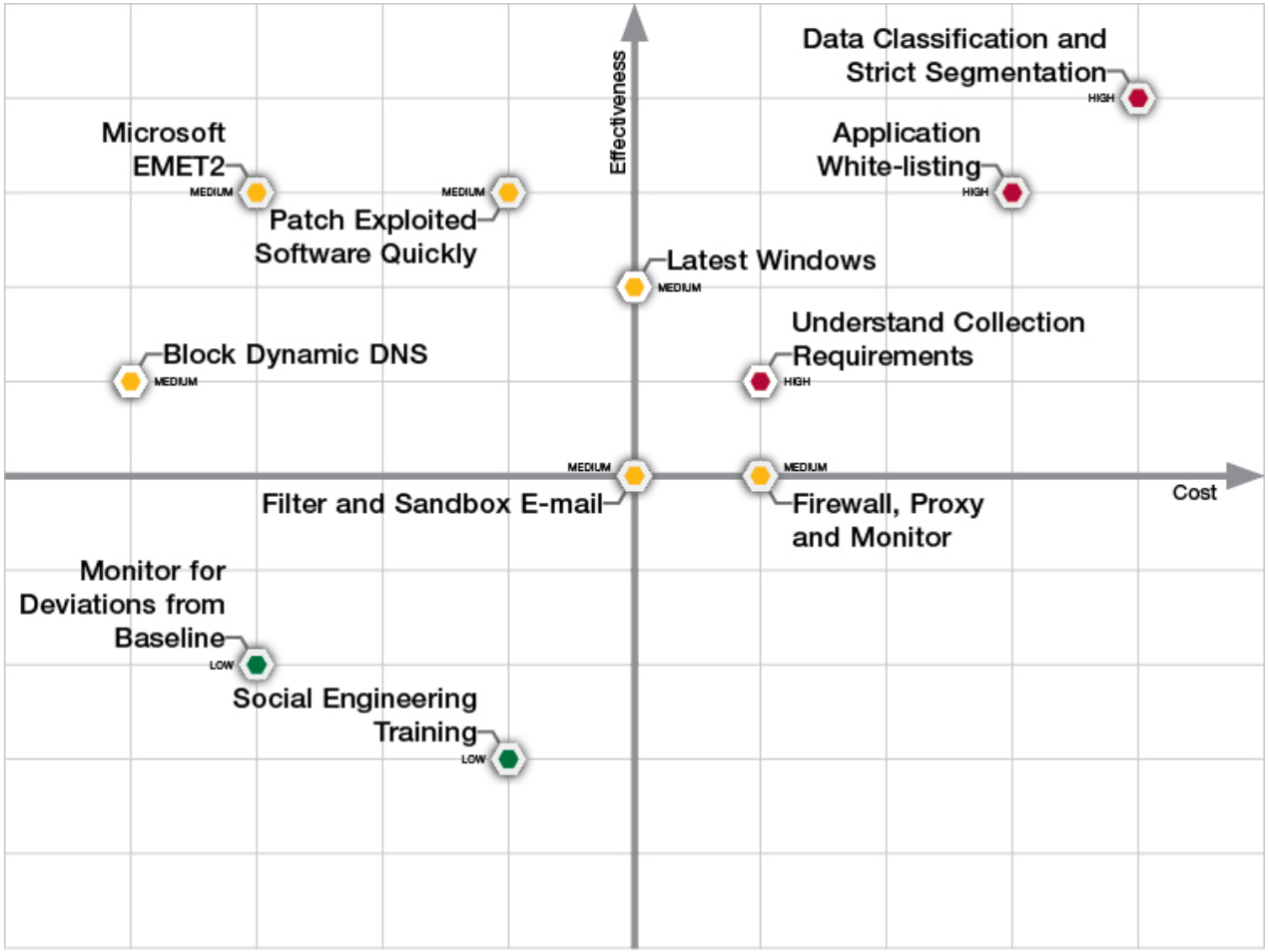
b) National Security

c) Foreign Policy

- Identify what assets are strategically important according to APT Collection Requirements
- Focus Enterprise IT Security resources on securing and monitoring these assets

INTERNET SECURITY ALLIANCE

Cost-Benefit Chart

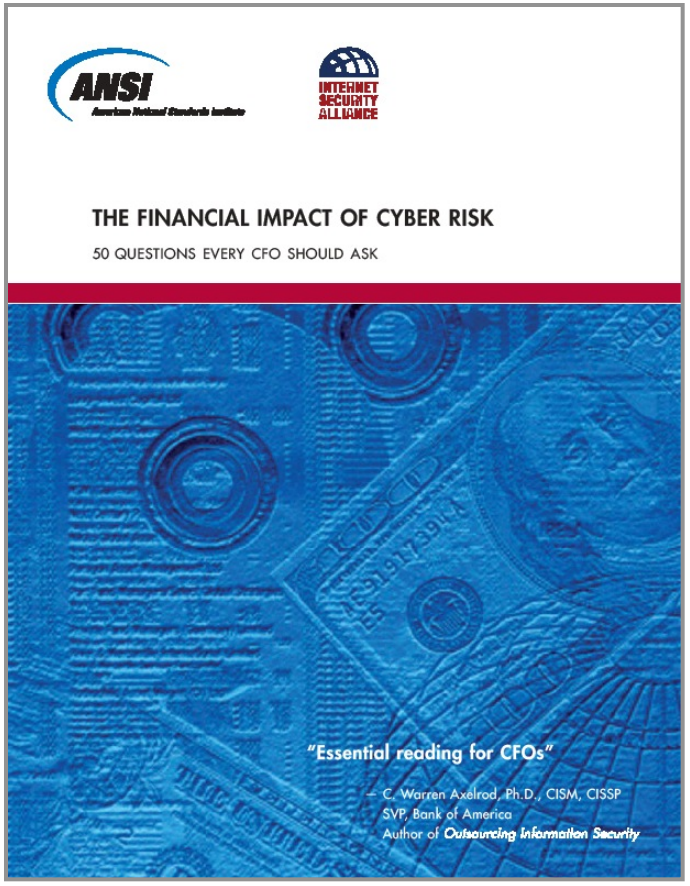


iDEFENSE

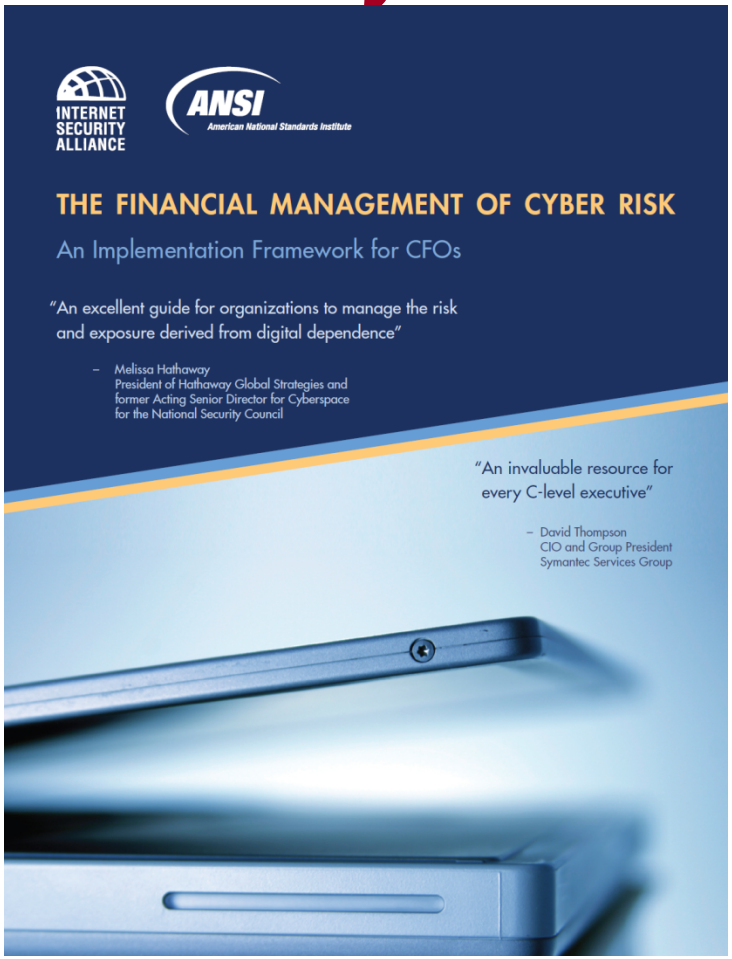
50 Questions Every CFO Should Ask (2008)

It is not enough for the information technology workforce to understand the importance of cyber security; 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. – President's Cyber Space Policy Review May 30, 2009 page 15

ISA-ANSI Project on Financial Risk Management of Cyber Events: "50 Questions Every CFO should Ask ----including what they ought to be asking their General Counsel and outside counsel. Also, HR, Bus Ops, Public and Investor Communications & Compliance



Financial Management of Cyber Risk (2010)

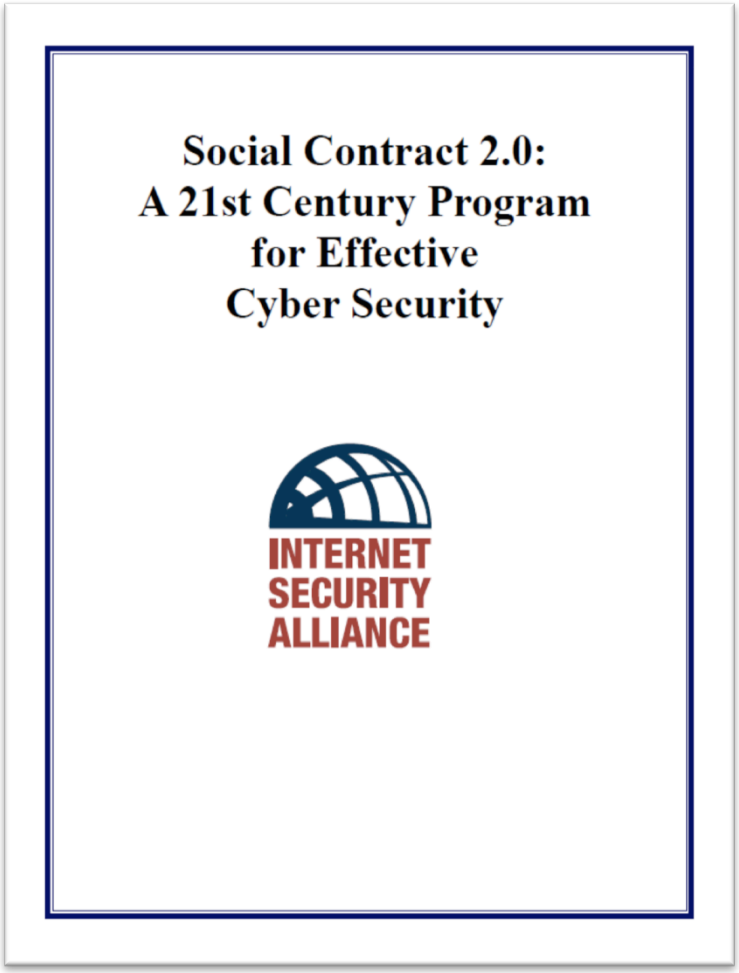


Growth toward Enterprise wide cyber management

DOE Risk management Framework

Senior executives are responsible how cyber security risk impacts the organization's mission and business functions . As part of governance, each organization establishes a risk executive function that develops an organization-wide strategy to address risks and set direction from the top. The risk executive is a functional role established within organizations to provide a more comprehensive, organization-wide approach. "

ISA Social Contract



Broad Industry and Civil Liberties Support

Improving our Nation's Cybersecurity through the Public-Private Partnership

A White Paper

Presented by

BSA Business Software Alliance · cdt Center for Democracy & Technology · Keeping the Internet Open • Innovative • Free · The Spirit of Enterprise U.S. Chamber of Commerce · Internet Security Alliance · TechAmerica Where the Future Begins

March 8, 2011

1

INTERNET SECURITY ALLIANCE

Two Types of Attacks

- Basic attacks
  - Vast majority
  - Can be very damaging
  - Can be managed
- Ultra-Sophisticated Attacks (e.g., APT)
  - Well organized, well funded, multiple methods, probably state supported
  - They **will** get in

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

- PWC/GI Inform 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

ISA-House Legislative Proposals

ISA Written Materials	Recommendations of the House Republican Cybersecurity Task Force
Menu of Market Incentives	***Menu of Market Incentives***
"To accommodate the needs of a wide variety of critical infrastructures with different economic models, the public-private partnership should develop a menu of incentives that can be tied to voluntary adoption of widely-accepted and proven-successful security best practices, standards, and technologies." *ISA President Larry Clinton's Written Testimony, June 24th before a House Homeland Security Subcommittee, p.4*	"We believe Congress should adopt a menu of voluntary incentives to encourage private companies to improve cybersecurity…" *Recommendations of the House Republican Cybersecurity Task Force, p.7*
One Size Does NOT Fit All	***One Size Does NOT Fit All***
"However, while it is true that one size of standards/ best practices may not apply equally well to various businesses or technology systems, it is also true that one set of incentives may have different applicability and attractiveness to different types of sizes of enterprises." *ISA Social Contract 2.0, p.16*	"We also have to recognize that different companies and sectors will need different incentives – one size does not fit all." *Recommendations of the House Republican Cybersecurity Task Force, p.7*

ISA-House Legislative Proposals

ISA Written Materials

Streamlined Regulation as an Incentive

Streamline regulations/reduce complexity. Regulatory and legislative mandates and compliance frameworks that address information security, such as Sarbanes-Oxley, Gramm-Leach-Bliley, the Health Insurance Portability and Accountability Act, along with state regimes, could be analyzed to create a unified compliance mode for similar actions and to eliminate any wasteful overlaps…

ISA Social Contract 2.0, p.16

Recommendations of the House Republican Cybersecurity Task Force

Streamlined Regulation as an Incentive

Streamline Information Security Regulations: … Congress could require the Administration to coordinate with critical infrastructure sectors to develop strong performance standards that, if a company was found compliant with the new standard, would satisfy the information security/privacy protections of SOX, HIPAA, GLB etc. A company would be encouraged to implement stronger security standards by allowing it to save money and time by avoiding multiple audits from multiple regulators.

Recommendations of the House Republican Cybersecurity Task Force, p.8

ISA-House Legislative Proposals

ISA Written Materials

Taxes and Grants

"*Tie federal monies (grants/SBA loans/stimulus money/bailout money) to adoption of designated effective cyber security standards/best practices...* **make on-going eligibility for federal contracts, grants and loans contingent on compliance with identified security practices. This is a proven, and successful, method for advancing broad policy objectives (e.g., non-discrimination in employment)...."**

ISA Social Contract 2.0, pp.16-17

"*Tax incentives for the development of and compliance with cyber security standards practices and use of technology...***tax credits can be made contingent upon compliance with established and pre-identified cyber security practices..."**

ISA Social Contract 2.0, pp.17-18

"*Grants/Direct Funding of Cyber Security R&D.* **The Federal Government could give grants to companies that are developing and implementing cyber security technologies or best practices..."**

ISA Social Contract 2.0, pp.17-18

Recommendations of the House Republican Cybersecurity Task Force

Taxes and Grants

"*Existing Tax Credits:* **To encourage companies to increase their investment in network security, Congress should consider expanding or extending existing tax credits, such as the R&D tax credit, to apply to cyber investments as an alternative to creating new tax credits.**

Existing Grant Funding: **Existing grant funding should be evaluated as an alternative to new funds. Congress could also evaluate including minimum cybersecurity protection standards in grant proposals for grantees dealing with issues such as national security, law enforcement, and critical infrastructures as a condition for receiving government funds. These would include general protection standards such as updating computer patches or running anti-virus software that would not be overly burdensome to grant recipients."**

Recommendations of the House Republican Cybersecurity Task Force, p.8

ISA-House Legislative Proposals

ISA Written Materials

Liability Protection

"*Limit liability for good actors.* **The Federal Government could create limited liability protections for certified products and processes... or those certified against recognized industry best practices. Alternatively, liability might be assigned on a sliding scale (comparative liability), such as limiting punitive damages while allowing actual damages, and providing affirmative defenses with reduced standards (preponderance of evidence vs. clear and convincing etc.).**"

ISA Social Contract 2.0, p.18

Regulation CANNOT Keep Up

The process of developing effective regulations is inherently time consuming there is virtually unanimous agreement that any regulations specific enough to assure improved cyber security would become outdated soon after their enactment.

ISA Social Contract 2.0, p.2

Recommendations of the House Republican Cybersecurity Task Force

Liability Protection

"If existing regulators are imposing a jointly developed cybersecurity standard, the company should be granted some level of liability protection for following this standard. To encourage compliance, regulated entities would be granted limited liability protection in the instance of a breach if they meet or exceed mandated standards. Compliance would be determined through oversight of existing regulators."

Recommendations of the House Republican Cybersecurity Task Force, p.9

Regulation CANNOT Keep Up

Threats and practices change so quickly that government-imposed standards cannot keep up.

Recommendations of the House Republican Cybersecurity Task Force, p.7

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

www.isalliance.org