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

Outline of Presentation

- The Evolving Cyber Threat
- The Economics of Cyber Security
- Enterprise Risk Management for Cyber Security
- Public Policy/Economics/Enterprise partnerships & Cyber Security

ISAlliance
Mission Statement

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

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 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

% 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.

The Cyber Security Economic Equation

- Technological analysis tells us HOW cyber attacks occur. Economics tells us WHY they occur
- 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

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

- National Strategy to Secure Cyber Space (2002) held that business efficiency would drive cyber security investment.
- DHS "Eco-system" Paper (2011) holds the same view
- Business efficiency demands LESS secure systems (VOIP/international supply chains/ Cloud)

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 I think 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

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

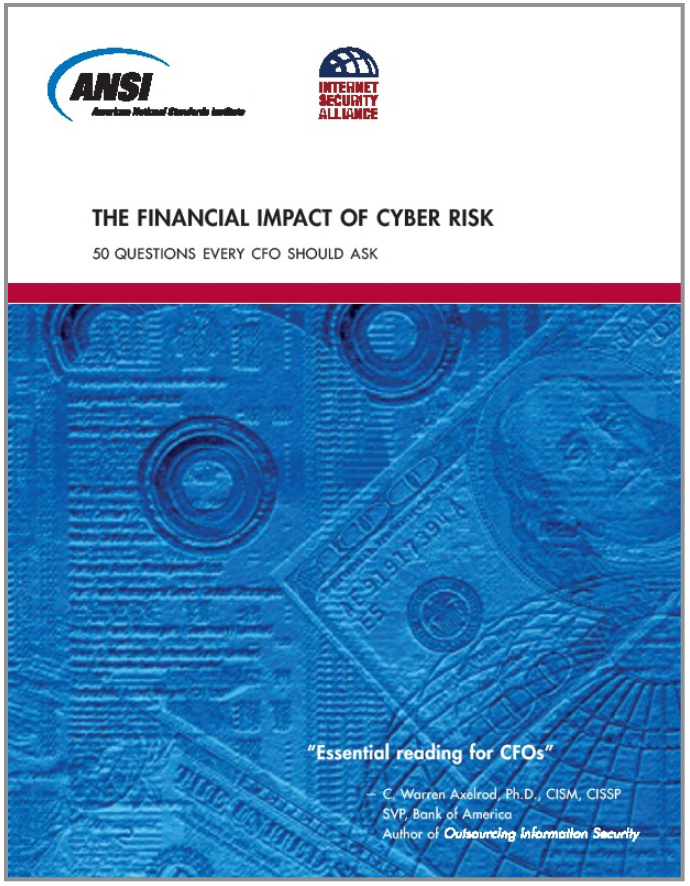
We are not cyber structured

- In 95% 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 US Companies are deferring or reducing investment in cyber security

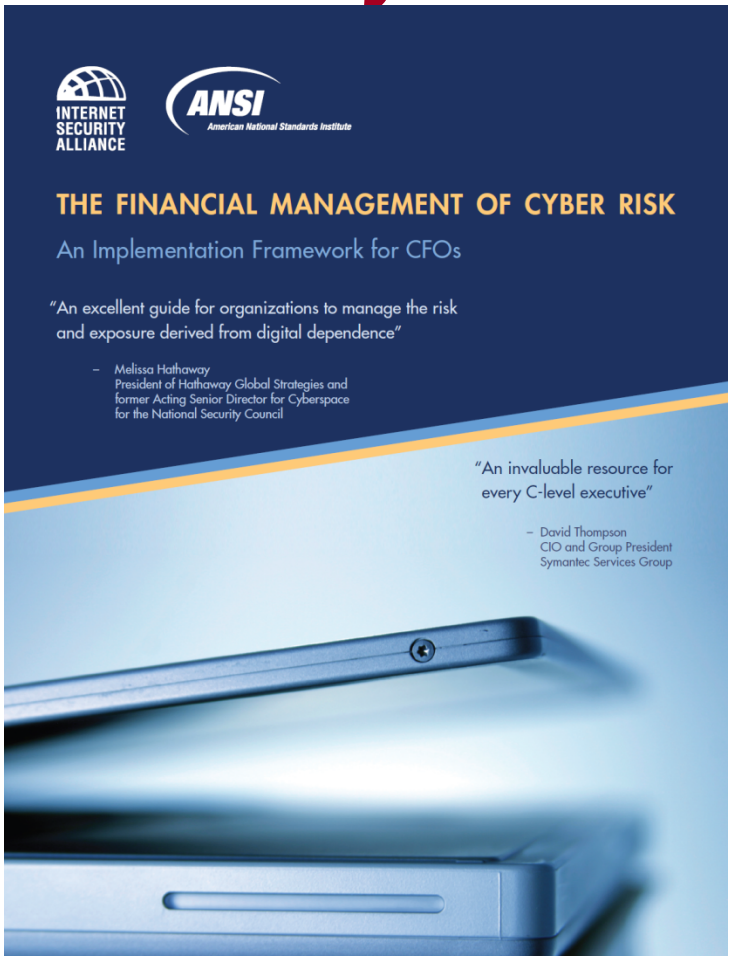
50 Questions Every CFO Should Ask (2008)

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)



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

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

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

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?

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?

Communications

- Do we have a plan for multiple audiences?

--general public

--shareholders

--Govt./regulators

--affected clients

--employees

---press

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?

Best Practices do Work

- 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

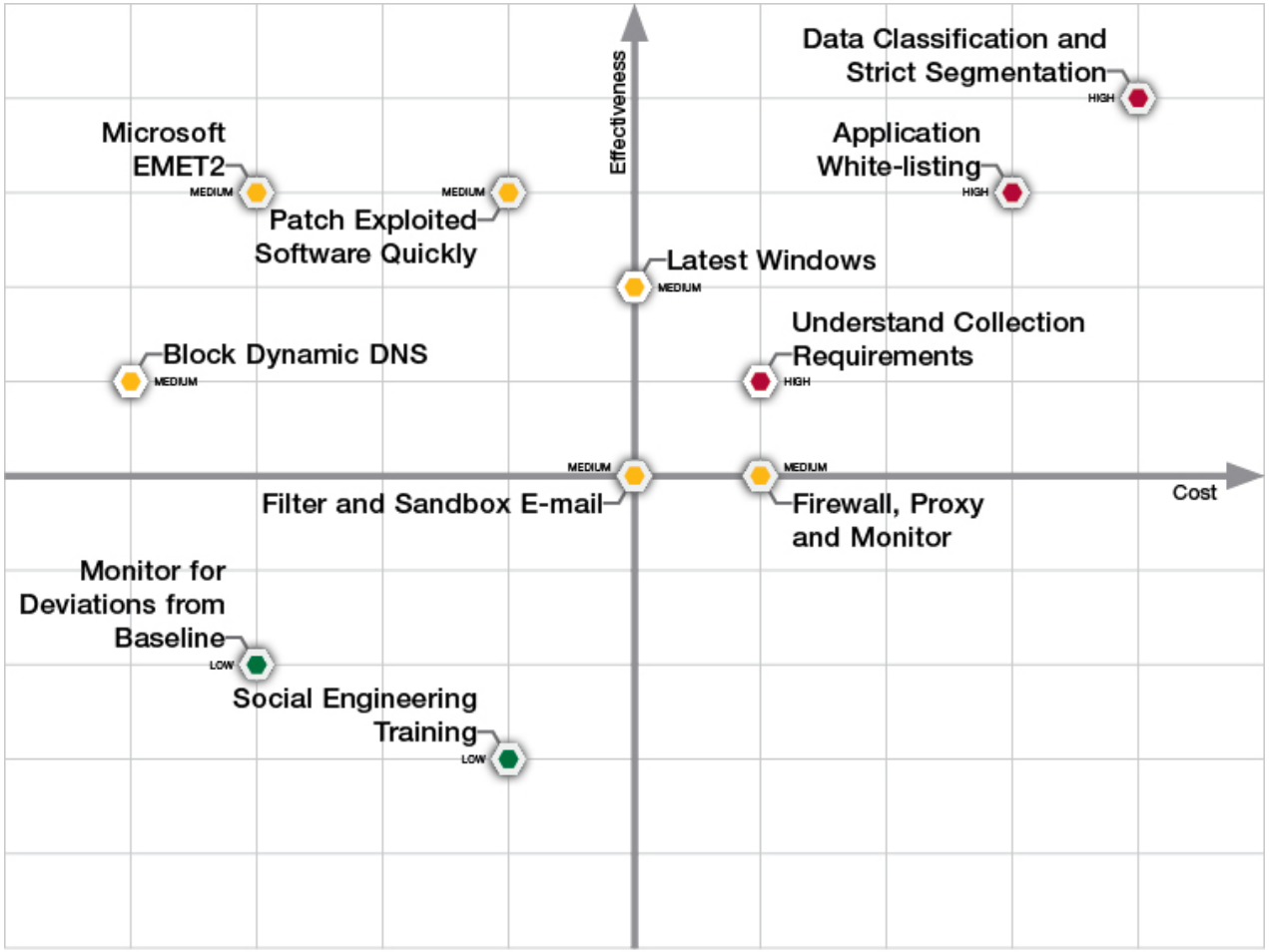
INTERNET SECURITY ALLIANCE

APT Best Practices

- Corporate Due Diligence
- Preventing and Identifying Exploitation
- Managing Outgoing Data Exfiltration
- Understand Why you are an APT Target

INTERNET SECURITY ALLIANCE

Cost-Benefit Chart



iDEFENSE

Growth toward Enterprise wide cyber management

- In 2008 only 15% of companies had enterprise wide risk management teams for privacy/cyber
- In 2011 87% of companies had cross organizational cyber/privacy teams
- Major firms (E & Y) are now including ISA Financial Risk Management in their Enterprise Programs
- Fed Agencies beginning to recognize the economic issues in CS----- e.g. SEC and DOE

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. "

Why APT is a Public Policy Issue?

"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

INTERNET SECURITY ALLIANCE

Public Policy Options

- Senate/Administration Proposals
- DHS should set regulations for Private Sector owners and operators
- Will the Regulatory Approach be effective?
- What are the economic implications of an extended regulatory policy on critical infrastructure innovation, investment and competitiveness?

Social Contract--Incentive Based Approach

- The Social Contract/ISA/Industry/Civil Liberties Approach ---market incentives to encourage owners & operators to voluntarily elect improved security
- House Task Force Approach----follows the social contract model
- Rogers bill---House Intel on info sharing
- Lungren Bill ---create a menu of incentives

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*

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

www.isalliance.org