The Value Proposition for Cyber Security: Does it exist and how can we create it?

Larry Clinton, ISAlliance
Chief Operating Officer
Who We Are
What we believe

- The World has Changed
- Globalization
- Digitalization
- Terrorism
- Traditional Regulatory Mechanisms won’t work
- Too slow
- US only
- Retard needed economic growth
Economic Effects of Attacks

- 25% of our wealth---$3 trillion---is transmitted over the Internet daily.
- FBI: Cyber crime cost business $26 billion (probably LOW estimate).
- Financial Institutions are generally considered the safest---their losses were up 450% in the last year.
- There are more electronic financial transactions than paper checks now, 1% of cyber crooks are caught.
“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
“The technology community has made much progress in the past 5 years improving technical security. Yet, moving the needle on information security is a team activity, The hardest remaining issues involve people and organizations.”

“Embedding Information Security into the Extended Enterprise.” Dartmouth University 2006
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
23% of CTOs did not know if cyber losses were covered by insurance or not.

34% of CTOs thought their 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
What needs to be Done?
Realize the Value Proposition

- Role for industry:
  - Determine how to solve the problem

- Role for Government
  - Encourage industry to adopt proven solutions
Can we mitigate cyber Attacks? YES

- PricewaterhouseCoopers conducted 2 International surveys (2004 & 2006) covering 15,000 corporations of all types

- Apx 25% of the companies surveyed were found to have followed recognized “best practices” for cyber security.
Benefits of Best Practices

- Reduces the number of successful attacks
- Reduces the amount of down-time suffered from attacks
- Reduces the amount of money lost from attacks
- Reduces the motivation to comply with extortion threats
Senior Mgrs Best Practices

- Cited in US National Draft Strategy to Protect Cyber Space (September 2002)
- Endorsed US India Business Council (April 2003)
IS ALLIANCE BEST PRACTICES

- Practice #1: General Management
- Practice #2: Policy
- Practice #3: Risk Management
- Practice #4: Security Architecture & Design
- Practice #5: User Issues
- Practice #6: System & Network Management
- Practice #7: Authentication & Authorization
- Practice #8: Monitor & Audit
- Practice #9: Physical Security
- Practice #10: Continuity Planning & Disaster Recovery
Why Doesn’t Everyone Comply with the Best Practices?

“Many organizations have found it difficult to provide a business case to justify security investments and are reluctant to invest beyond the minimum. One of the main reasons for this reluctance is that companies have been largely focused on direct expenses related to security and not the collateral benefits that can be realized”

---Stanford University ‘06
Management is WRONG

Stanford Global Supply Chain Management Forum/IBM Study:

“Clearly demonstrated that investments in security can provide business value such as:

* Improved Product Safety (38%)
* Improved Inventory management (14%)
* Increase in timeliness of shipping info (30%)
There’s More !!!

- Increase in supply chain information access (50%)
- Improved product handling (43%)
- Reduction in cargo delays (48% reduction in inspections)
- Reduction in transit time (29%)
- Reduction in problem identification time (30%)
- Higher customer satisfaction (26%)
Security, like Digital Technology must be Integrated in Bus Plan

“Security is still viewed as a cost, not as something that could add strategic value and translate into revenue and savings. But if one digs into the results there is evidence that aligning security with enterprise business strategy reduces the number of successful attacks and financial loses as well as creates value as part of the business plan.”

PricewaterhouseCoopers Sept 2006
Key Issues for Industry

- Globalization and outsourcing have increased the challenges of security.
- Security metrics must be more tightly linked to the business.
- Investment in security must move from reactive add-ons to proactive initiatives consistent with company’s strategic goals.
- Directives must come from the top.

Dartmouth University 2006
AIG developed an on-line metric tool based on ISAlliance Best Practices for Senior Managers

- Separate tool developed for small businesses based on small business best practices
- Qualified companies can receive up to 15% discount on cyber insurance
ISA Security Integration Program - Get the team involved

- Issues must be addressed simultaneously from the:
  - Legal
  - Business
  - Technology
  - Policy
  - Perspectives
ISAlliance Integrated Business Security Program

- Outsourcing
- Risk Management
- Security Breach Notification
- Privacy
- Insider Threats
- Auditing
- Contractual Relationships (suppliers, partners, sub-contractors, customers)
Things Government Can Do

- Stimulate the insurance market
  - Temporary insurer of last resort (e.g. w/crop and flood insurance)
  - Use government’s market power (e.g. require contractors to have insurance)
  - Civil Liability reform (Precedent: Anti-Terrorism Act of 2002)
  - Allow info sharing to create better metrics (e.g. Y2K)
More for Government to do

- Create Gov/Industry/Education Consortium (e.g. Sema-Tech)
- Create Awards Programs (e.g. Baldridge Awards for Quality)
- Develop Significant outreach programs targeted at senior corporate execs.
Larry Clinton

Chief Operations Officer
Internet Security Alliance
lclinton@isalliance.org

703-907-7028 (O) 202-236-0001 (C)