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
- 5000 examples of malware created
- 2 million dollars lost

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

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

Cyber Security in India

"While other countries have reported enormous loses due to cyber crime…there are hardly any such reports coming out of India. Much of this success is attributed to work by NASCOM'S Data Security Council and National Skills Registry and the assigning of Sr. policy officials to assist NASSCOM"

Some cause for concern

- India's National Crime Records Bureau reports a 50% increase in cyber crime in one year
- India is the 3rd largest producer of SPAM
- The % of worms and viruses in India is significantly higher than any the Asian Pac Rim average
- India ranks second in web based attacks among the Asian Pacific Rim countries

Long term problems for India

As in most other countries around the world the cyber security situation in India is one of relative chaos and insecurity arising from periodic reports of espionage, cyber terrorism cyber warfare, and cyber crime. The complexity of the issue has resulted in a virtual a paralysis. Legal and law enforcement mechanisms have not shifted gears fast enough…lack of a coherent policy will seriously interfere with India's national security and economic development."

Criminals are winning

"A vast underground economy has resulted in an explosion of zero day vulnerabilities, attack tool kits and botnets. The vast sums of money cyber criminals receive has led to malicious code, worms and Trojans of increased sophistication leading to ever increasing fraud and espionage…India's approach to cyber crime thus far has been piecemeal with many organizations but little definition of roles, responsibilities or synergies of action."

INTERNET SECURITY ALLIANCE

If Your Thinking..

- Breaches and perimeter defense…
- Hackers…
- Going after networks…
- You are thinking all wrong!

If Your Thinking Tech..

- An Enterprise Wide Risk Management Issue
- Technology without economics is as misguided as thinking of economics without technology
- Tech tells us HOW attacks occur, economics tells us WHY attacks occur
- The single biggest threat is from insiders

INTERNET SECURITY ALLIANCE

What are the Roles in the Digital Age?

- Digitalization changes everything….notions of privacy/notions of defense and economics
- What is the proper role for government?
- What is the proper role for the military
- What is the proper role for industry
- How can a sustainable public private partnership evolve
- What is YOUR role?

Back to Basics

- What is the problem we are trying to solve?
- What is preventing us form solving the problem?
- How do we approach this problem in a risk management framework?

INTERNET SECURITY ALLIANCE

Regulation wont work

- Technology Changes too quickly.
- Attack methods change too quickly
- Gov. process will be political and minimal
- Problem is international---beyond any govt & international governance is impractical
- Name and shame creates incentive not to look and could incentive to incentives to attack
- Audits may not improve security could be counter productive

Internet Security Alliance Mission

ISA seeks to integrate advanced technology with 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

Cyber Security and the 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"

INTERNET SECURITY ALLIANCE

Cyber Economic Equation: Incentives Favors Attackers

- Offence: Attacks are cheap
- Offence: Attacks are easy to launch
- Offence: Profits from attacks are enormous
- Offence: GREAT business model ("resell" same service)

- Defense: Perimeter to defend is unlimited
- Defense: Is compromised – hard to show ROI
- Defense: Usually a generation behind the attacker
- Defense: Prosecution is difficult and rare

INTERNET SECURITY ALLIANCE

Business Efficiency Hurts Security

- Business efficiency demands less secure systems
- VOIP
- international supply chains
- BYOD
- Cloud computing
  THE MORE SECURE YOU MAKE THESE SYSTEMS
  THE LESS ECONOMIC THEY ARE

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"

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

Research from Pricewaterhouse/US Secret Service/Verizon Between 80---94% of cyber attacks can be stopped or mitigated by adopting inexpensive best practices and standards that already exist in the market

Why are We not doing it?

"The challenge in cyber security is not that best practices need to be developed, but instead lies in communicating these best practices, demonstrating the value in implementing them and encouraging individuals and organizations to adopt them."

The Information Systems Audit and Control Association (ISACA)- March 2011

INTERNET SECURITY ALLIANCE

Why are We not doing it?

- "Overall, cost was most frequently cited as "the biggest obstacle to ensuring the security of critical networks."
- "Making the business case for cyber security remains a major challenge, because management often does not understand either the scale of the threat or the requirements for a solutions."
- "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." ----from CSIS & PWC Surveys 2010

A 21st Century Social Contract

- Since the problem is economic we need an economic solution
- A cost effective approach will not only provide immediate help but offers a sustainable solution
- ISA SOCIAL CONTRACT----rely on industry standards and practices & Government provides economic incentives to voluntarily adopt
- Adopted by House GOP & now Obama Administration in Executive Order

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 who do don't consider cyber in the plan
- In 2009 & 2010, 50%-66% of companies deferred or reduced investment in cyber security

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 CFOs Need 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 enterprise-wide feedback

INTERNET SECURITY ALLIANCE

What we can do---APT

- Understand this is not your father's attack
- Adapt or strategy from perimeter defense to generic attacks to internal analysis, and remediation, new methods, new metrics
- For Example the "Roach Motel" Model for info sharing w/new roles and incentives
- Adapt big data analytics to cyber security

Larry Clinton

President & CEO
Internet Security Alliance

lclinton@isalliance.org

703-907-7028

202-236-0001

www.isalliance.org