For information about membership opportunities, please contact:

Larry Clinton
President & CEO
lclinton@isalliance.org
(703) 907-7028

For more information about the Internet Security Alliance, please visit www.isalliance.org
The Cybersecurity Story
The Cyber Security Story

- The Problem
- Urgency
- Barriers to Resolution
- The Champion
- The Resolution
Problem
In the last minute.....

- 5,500 records were lost due to cyber crime
- $4,400 dollars were lost due to cyber crime
- 832 versions of new malware were created
How Good are our defenses?

The military’s computer networks can be compromised by low to middling skilled attacks. Military systems do not have a sufficiently robust security posture to repel sustained attacks. The development of advanced cyber techniques makes it likely that a determined adversary can acquire a foothold in most DOD systems and be in a position to degrade DOD missions when and if they choose.” Pentagon Annual Report Jan 2015.
Barriers
We don’t understand the problem

• Hackers?
• Just Credit Cards and PII
• I’m safe or They Don’t Care about me
• Breaches?
• Firewalls and passwords?
• Networks?
• Perimeter Defense---keep the bad guys out
• If your thinking just IT.....
We don’t understand the problem

- 80% of CEOs are “very confident” – but successful compromises up 66%
- 71% of attacks are on firms w/less than $2 billion who don’t have the economies of scope and scale
- CEOs still prioritize keeping the bad guys out
- We don’t have enough people
- The “solutions” are making the problem worse
Additional Barriers

• The system is inherently weak
• Our laws and systems were not designed for the digital age
• We can’t secure ourselves (interconnection)
• We don’t want to pay for security
• All the economic incentives favor the attacker
• We are not cyber structured
Urgency
Things are going to get worse … much worse

- The system is getting even weaker

- The attackers are getting much better

- The real crazies could become a real threat
Champion
Government
Kremlinology
Copies of ISA’s Cybersecurity Social Contract can be obtained online at Amazon.com.
Copies of the ISA/NACD Cyber-Risk Oversight Handbook can be obtained at:
http://www.isalliance.org/cyber-risk-handbook
5 NACD Principles

- Cyber Security is not an IT issue
- You must understand your unique legal responsibilities
- You need to have access to adequate cyber security expertise
- Management must have a cyber security framework (a plan)
- You must systematically analyze your cyber risks (what to you accept, eliminate, mitigate, transfer?)
“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 Cyberspace Policy Review.

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.
THE FINANCIAL MANAGEMENT OF CYBER RISK

An Implementation Framework for CFOs

"An excellent guide for organizations to manage the risk and exposure derived from digital dependence"
- Melissa Hathaway
  President of Hathaway Global Strategies and
  former Acting Senior Director for Cyberspace
  for the National Security Council

"An invaluable resource for every C-level executive"
- David Thompson
  CIO and Group President
  Symantec Services Group
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
Appendices/Tools for the Board of Directors

• Questions to ask Management
• Supply Chain Risk (Vendor Management)
• Metrics
• M&A Risks
• What to Expect from Government
• Sample Dashboard
• Building a Relationship with the CISO
• Insider Threats
Corporate Boards are getting involved

• Guidelines from the NACD advise that Boards should view cyber-risks from an enterprise-wide standpoint and understand the potential legal impacts. They should discuss cybersecurity risks and preparedness with management, and consider cyber threats in the context of the organization’s overall tolerance for risk. -- PWC 2016 Global Information Security Survey
Boards are taking action

- Boards appear to be listening to this advice. This year we saw a double-digit uptick in Board participation in most aspects of information security. Deepening Board involvement has improved cybersecurity practices in numerous ways. As more Boards participate in cybersecurity budget discussions, we saw a 24% boost in security spending. --- PWC 2016 Global Information Security Survey
Actual Cyber Security Improvements

- Notable outcomes cited by survey respondents include identification of key risks, fostering an organizational culture of security and better alignment of cybersecurity with overall risk management and business goals. Perhaps more than anything, Board participation opened the lines of communication between the cybersecurity function and top executives and directors -- PWC 2016 Global Information Security Survey
1. These proposed engagements are assessments, not audits.
2. Measuring cyber assessments should use a maturity model.
3. Cybersecurity is not all about “IT”.
4. Assessment tools need to focus primarily on techniques with proven effectiveness and cost effectiveness.
5. The assessment tool needs to be a voluntary model – really voluntary.
6. We need to assure there will be adequate Talent Availability to perform the assessments.
Resolution
All We Need to Do is …

- Understand the problem better
- Alter the fundamentals of digital economics
- Modernize our laws and law enforcement efforts
- Develop a Cyber aware work force
- Change our corporate structures and evaluation methods
- Engage our government partners in a joint effort against the bad guys
Champion