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
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.
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
Government
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
How to think about cyber security (for boards)

• THE BAD NEWS: You can’t “solve” the cyber security problem

• THE GOOD NEWS: You can manage your cyber risk

• Think of cyber as you think of your personal health...no one lives germ free
Different Kinds of Cyber Risk for Corporations

• Data security risk—loss/corruption of data/Intel Prop/Bus Plans etc.

• Legal Risks ---e.g. class action/violation of fiduciary duty

• Reputation Risk ---will anyone do business with you ---are you inviting regulatory scrutiny?
5 NACD Principles

- Cyber Security is not an IT issue
- Boards must understand their unique legal responsibilities
- Boards 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?)
Principle 1 Cyber is Not an IT Issue (Sec/Rep)

• The threat is not just from the outside
  -- Insiders/Vendors/Customer

• Cyber should be considered as a part of core business decisions-M & A/Product Development/PR

• IT is in an inherently conflicted position to provide the information you need
Principle 2. Legal Issues (compliance)

• Legal liability for cyber is unsettled and varies with the business & location

• "companies affected by data breaches have come to expect class-action suits [against corporate boards of directors] filed by consumers alleging privacy violations and unwarranted disclosure of their personal identification information... these cases indicate that litigation costs for companies affected by large-scale data breach events will continue to increase because the plaintiffs’ bar has added shareholder lawsuits to its collective response to breach events."

• Consult with outside counsel
Principle 3. Adequate Cyber Expertise (Sec)

- Do you have legal and finance experts? --- what business decisions don’t include cyber? —do you need to add expertise?
- Get regular reports from management
- CISO direct communication with the board
- Schedule regular “deep dive” briefings
- Director education programs
- Time and relationships with Law Enforcement
“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
Symmetric 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
P5. Define risks to accept, mitigate, transfer (Sec)

- What data, and how much are we willing to lose/compromise?
- How to divide cyber security investments between basic and advanced defenses?
- What options are available to transfer risk?
- How should we assess the impact of cyber events?
Appendices/Tools for the Board of Directors

- Questions to ask Management
- Supply Chain Risk (Vendor Management)
- Insider Threats
- Metrics
- M&A Risks
- What to Expect from Government
- Sample Dashboard
- Building a Relationship with the CISO
Building a Relationship w/ the Board & Management

- Make sure they understand your role
- Engage them BEFORE an incident occurs
- Make sure they understand how you work with the rest of the organization
- Make sure success is evaluated the proper way
- Generate discussions about the state of the organization as a whole
Champion