INTERNET
SECURITY
ALLIANCE

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

www.isalliance.org

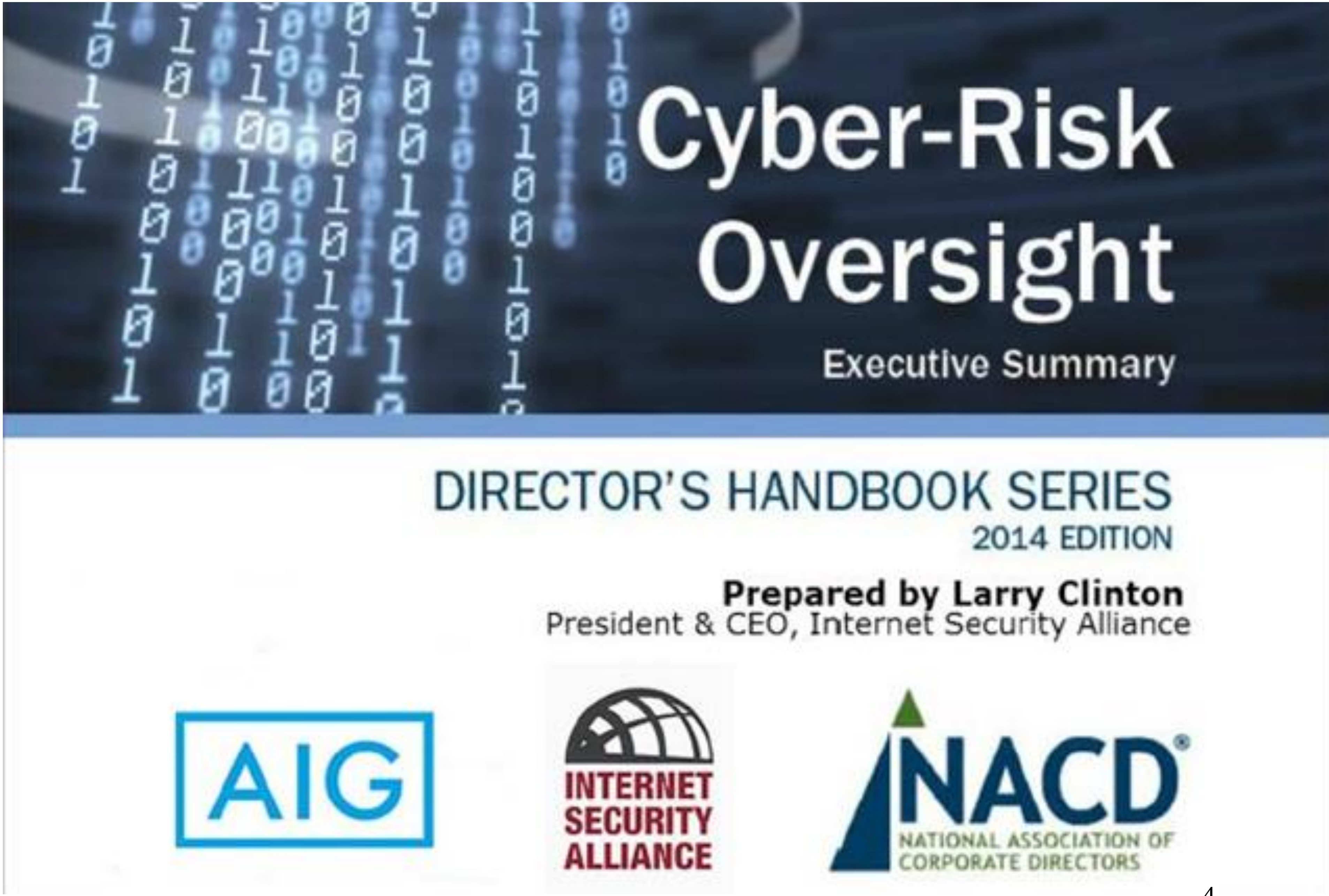
Are You as Safe as DoD?

"The military's computer networks can be compromised by **low to meddling 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.

INTERNET SECURITY ALLIANCE

Things are getting worse

- The system is getting technologically weaker
- The attack community is getting (much) better
- The economics all favor the attackers



Cyber-Risk Oversight

Executive Summary

DIRECTOR'S HANDBOOK SERIES
2014 EDITION

Prepared by Larry Clinton
President & CEO, Internet Security Alliance

AIG

INTERNET
SECURITY
ALLIANCE

NACD®
NATIONAL ASSOCIATION OF
CORPORATE DIRECTORS

Does Following the Handbook work? -- YES

"Guidelines from the National Association for Corporate Directors (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.

Boards appear to be listening to this guidance. This year we saw a double-digit uptick in Board participation in most aspects of information security. Respondents said this deepening Board involvement has helped improve cybersecurity practices in numerous ways. It may be no coincidence that, as more Boards participate in cybersecurity budget discussions, we saw a 24% boost in security spending.

Additional Effects of NACD Handbook

“ Other 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, however, Board participation has opened the lines of communication between the cybersecurity function and top executives and directors..

Good News and Bad news…Bad news first

- THE BAD NEWS: You can't "solve" the cyber security problem
- THE GOOD NEWS: You can **manage** cyber risk
- Think of cyber as you think of your personal health…no one lives germ free.. But you can be healthy
- Just as all board business decisions have finance and legal aspects, in the digital age they have cyber aspects also.

Different Kinds of Cyber Risk for Corporations

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

- Reputation Risk ---will anyone do business with you ---are you inviting regulatory scrutiny?

- Actual security risk—loss/corruption of data/Intel Prop/Bus Plans etc.

5 Core Principles for Board to Follow

- Cyber is not an “IT” issue –Its an Enterprise Wide Risk Management business issue
- Understand the varying legal environments
- Access experts and provide adequate time for consideration of cyber issues
- Direct management to develop a framework for dealing with cyber (& test it)
- Management must identify risks to avoid, accept, mitigate, transfer

P 1. Not an IT Issue

- IT is in an inherently conflicted position
- 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
- IIA recommends annual full check of all cyber systems "SOX provides little assurance of security"

P 2. Understand Legal Issues of Cyber Risk

- 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

Some good news….

- The vast majority of consumers data breach lawsuits get dismissed after judges rule that the “plaintiffs' bar” has failed to prove the defendants suffered actual or threatened injury.” (Gov Info Security 5/15/15)

- But that could change……

Legal Issues

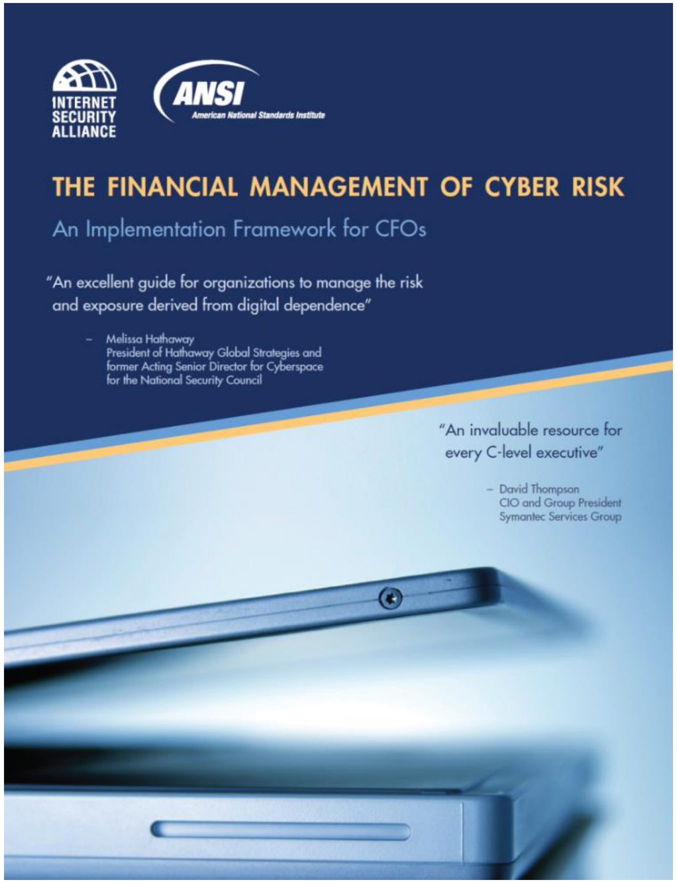
- SEC Guidance ---not a rule, but they can audit and investigate & might be useful in litigation. Consider probability, frequency severity, costs, adequacy of prevention outsourced functions, insurance coverage.
- Boards need to keep records
- Consult w/outside counsel---keep communications privileged

P 3. Have Adequate Expertise

- Do you have legal and finance experts? --- what business decisions don’t include cyber?
- Add cyber expert to the board, or leverage outside experts
- Schedule regular “deep dive” briefings
- Director education programs
- Get regular reports from management
- Relationships and time with LE & CISO

INTERNET
SECURITY
ALLIANCE

P 4 Cyber Framework NIST/ISA-ANSI



INTERNET
SECURITY
ALLIANCE

ANSI
American National Standards Institute

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

What does "Cyber Security" Mean to ….

- IT (NIST/SANS top 20)
- Human Resources
- Finance/M & A
- Operations/Plant management
- Legal and Compliance
- External Communications/PR
- Risk Management

P4. Expect Management to use a CS Framework

- Cross departmental person (e.g.: COO/CFO) in charge ---NOT IT
- Cross organizational team with all business units
- Meet regularly to develop reports to the board—track and report metrics/threat risk management & bus impact
- Organization-wide risk strategy & communication plan
- Total cyber risk budget

Cyber Risk Balance Sheet --- Assets

- Differentiate between “crown Jewels” and other data requiring lesser protection
- Strategy –People Process Technology

---People: Train. Limit to access/turn off w/termination, hire w/care SR MANAGERS!!!!

-- Process: Have good cyber hygiene/Chain of Trust for Vendors/BYOD policies for staff

---Tech: Know where your data is including at rest and in transit Encryption.

Liabilities

- Mobile Devices
- Cloud Computing
- VOIP
- IoT (Internet of Things)
- Data sprawl
- BYOD
- Long International Supply Chains
- M & A

Reputation is about PR

- Have a (tested) Plan
- What happened
- What are you doing about it?
- What are you doing so it will never happen again?

P.5 Man lays out risks to accept, mitigate, transfer

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

Accept ?Mitigate ? Transfer?

- What can/can't you afford to lose? (Public info? Redundant info? Proprietary info?)

- What losses can you anticipate and quantify?

(legal fees? Call center? Credit monitoring?)

- How much insurance do you need? (Can you get?) –Target's net loss? .01 annual sales

Handbook Vol.2 – New Sections on ….

- Proper metrics for the board
- Mergers and Acquisitions
- What Can we Expect from our Government Partners
- Building a Relationship between the board and the CISO

- SUPPLY CHAIN AND VENDOR MANAGEMENT

SC Questions for the Bd

- How do we balance $ with increased cyber risk?
- How much visibility do we have of our SC?
- What do we need to do to integrate CS into SC
- How is CS built into contracts & enforced?
- How hard and $ will it be to have pen testing of SC
- How hard & $ to enhance monitoring of SC?
- Do vendor agreements bring new compliance risk ?
- Are we indemnified 4 incidents by vendors?

The small company problem & how to solve it

- Supply chains used to reduce cost
- Supply chains are long and disparate
- Regs & Quasi regs have grown & cost exploded
- Many small companies can’t – or won’t comply
- Not everyone needs to be at the same level of compliance -- but that is how we measure it
- Cyber “Audits” are pass fail – Cyber security isn’t
- No proven link between compliance & security

Reform Cyber Audits & Supply Chain Regs

- Cyber “audits” are not audits
- Cyber assessments should be on a maturity model
- A maturity model will create greater prioritization
- A maturity will allow more small companies to participate leading to innovation
- A maturity model creates an incentive structure for smaller firms to enhance security
- ISA-CAQ and AICPA are working in this direction

INTERNET
SECURITY
ALLIANCE

Larry Clinton

President & CEO
Internet Security Alliance

lclinton@isalliance.org

703-907-7028

202-236-0001

www.isalliance.org