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 Cyber Security Story

- The Problem
- Urgency
- Barriers to Resolution
- The Champion
- The Resolution

Problem

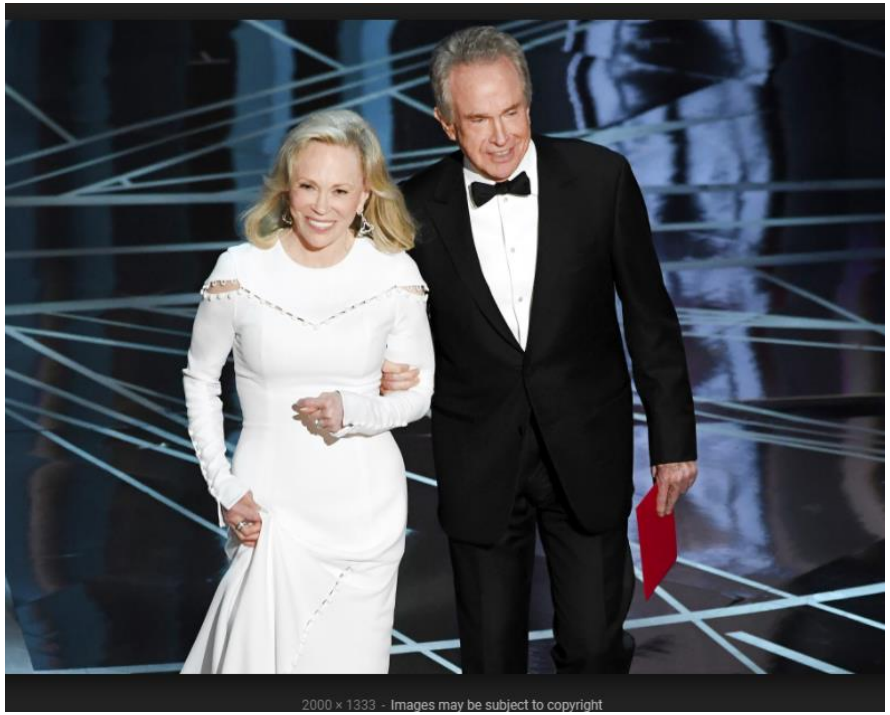
A History of the Problem

A BRIEF HISTORY OF

TECHNOLOGY USE AND

BANK CRIME

INTERNET SECURITY ALLIANCE



Cyber Crime: The numbers

- Costs: Hundreds of billions to a trillion dollars a year or more $445B just in Financial services. Up 30% last year
- One major ISP reports it sees 80 billion malicious scans a day
- 300 million new malicious viruses are created every day
- Financial Institutions report 3 attacks every second
- There were 4.8 billion records lost due to data breaches in 2016
- There are 4000 Ransomware attacks every day
- $200,000 per minute spent regulations and audits

Are we prepared

- 85% FS say cyber security function does not fully meet their needs
- 48% have no, or informal, threat intel program
- 54% have cyber function in IT
- 12% feel its very likely they can detect a sophisticated cyber attack
- 43% of boards have sufficient knowledge for effective cyber oversight

Is it the Technology or the Incentives?

"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"

Urgency

Things are getting worse Fast: Part I Weak Networks

- I-Net was designed to be “open” i.e. insecure
- Explosion in the use of mobile devices
- Consumers don’t “want” (to pay) for security
- BYOD (Bring Your Own Device) puts corporate security in individual’s hands
- The IoT is here …. The Internet of Things --- fax machines, security cameras, refrigerators – all new pathways for attacks and generally don’t have the capacity for security

Things are Getting Worse Fast: Part II–Attackers Getting better

- Well funded;
- Well organized---state supported;
- Highly sophisticated---NOT “hackers”;
- Thousands of custom versions of malware;
- They play the misdirection game;
- Escalate sophistication to respond to defenses;
- Maintain their presence and “call-home”;
- They target vulnerable people more than vulnerable systems.

Change the play (SWIFT)

- As protection of customers has improved criminals shift toward targeting the business (eg ATMs)
- PoS (down 90%) and card theft down shift to mobile banking attacks (up 300% since 2016)
- Protection in US shift to developing world – which is interconnected to US
- ATP now means average persistent threat
- A different kind of Phish – pre-texting/DOSS-IoT

How Good Are the Bad Guys?

"Cyber criminals are technologically as sophisticated as the most advanced IT companies and like them have moved quickly to adopt AI, cloud, software-as a service (cybercrime-as-a service) and encryption."

-- Symantec 2018 Cyber Crime Report

Getting Worse Fast Part III: Economics Favor Attacks

- Attacks are Cheep
- Attacks are Easy to Access
- Attacks are VERY PROFITABLE
- Great business model
- The system is inherently vulnerable
- Defense is a generation behind the attacker
- It's hard to show ROI on what you prevent
- Virtually no law enforcement

Put Succinctly…..

"Cybercrime is relentless, undiminished and unlikely to stop. It's just too easy, rewarding and the chances of getting caught are far too low. Cyber crime also leads on a risk to payoff rate. It is a low risk crime with high profits. A smart cyber criminal can easily make millions without fear of being caught."

-- McAfee 2018 Cyber Crime Report

Barriers

Barrier: Complex technology is changing the game

- It is now becoming obvious that the accelerating pace of technological change is the most creative force—and also, the most destructive one—in the financial services ecosystem today –

  -- PWC Global Information Security Survey 2017

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.

The real cyber challenge is the economics

"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

Digital economics are not obvious

"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"

Barrier: Old Models Don't work vs new threats

Many financial institutions still rely on the same information security model that they have used for years: one that is controls- and compliance-based, perimeter-oriented, and aimed at securing data and the back office. But information security risks have evolved dramatically over the past few decades, and the approach that financial institutions use to manage them has not kept pace.

-- PWC Global Info Security Survey 2017

Traditional vs Leading Edge Cyber Risk Management

- Checking boxes --- the more you check the more mature you are and hence the more secure, right?
- Which unchecked box do we focus on?
- How much risk reduction do we get from checking one box over the other?
- What's the difference between yellow and green? (3 and 4?) … garbage in … garbage out
- We need prioritization, cost based, empirical

Problems with Traditional Cyber Risk Assessment

- People (even “experts”) have different meanings for terms like “likely” “probable” “unlikely” “extremely unlikely”
- Things like heat maps imply certainty but can’t tell you:
- How much money you will lose ?
- How probable the scenario is ?
- What is the adequate risk reduction cost ?

Problems with Traditional Cyber Risk Assessment – It doesn't work

"There is not a single study indicating that the use of such methods actually reduces risk."

Doug Hubbard How to Measure Anything in Cyber Security

Start at the beginning: What is a Risk?

- Insiders?
- Supply Chain?
- Mobile Technology?

How much risk is there?

A little

None

A lot

How much risk is there?

A little

None

A lot

How much risk is there?

A little

None

A lot

What Is Risk

- Risk is best conceptualized as a quantity. It is a measure of future loss from a given scenario representing how much money an organization might lose from a given scenario over time

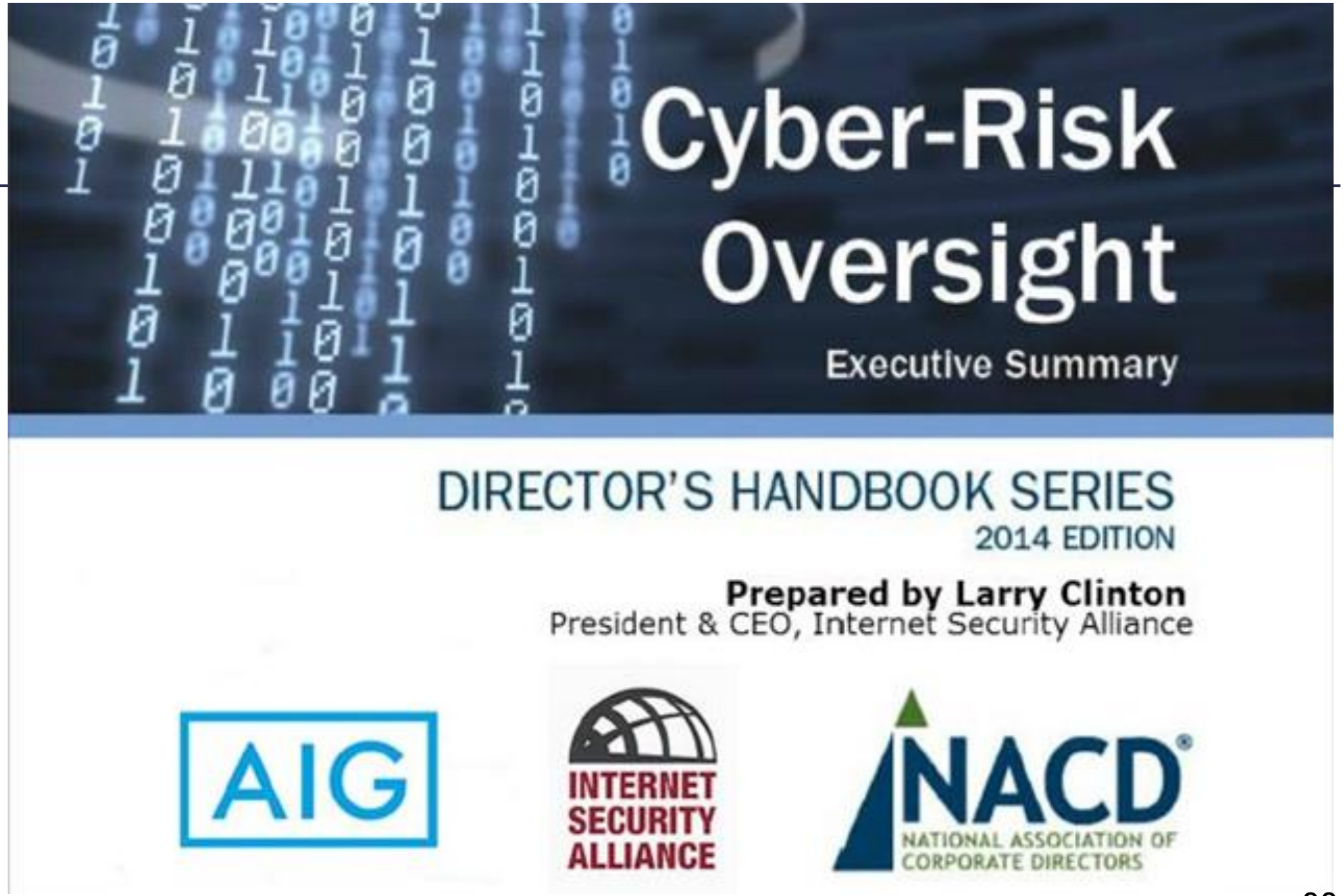
We Need to put Cyber Risk in Economic terms to manage it

- "Overall, cost was most frequently cited as "the biggest obstacle to ensuring the security of critical networks." -- PWC
- "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." -- McAfee
- "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 in business terms." -- CSIS

Heroes

INTERNET SECURITY ALLIANCE

Government


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

New Approach to Cyber Security: Start at the top

- 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

Actually Involving the Board helps

- 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

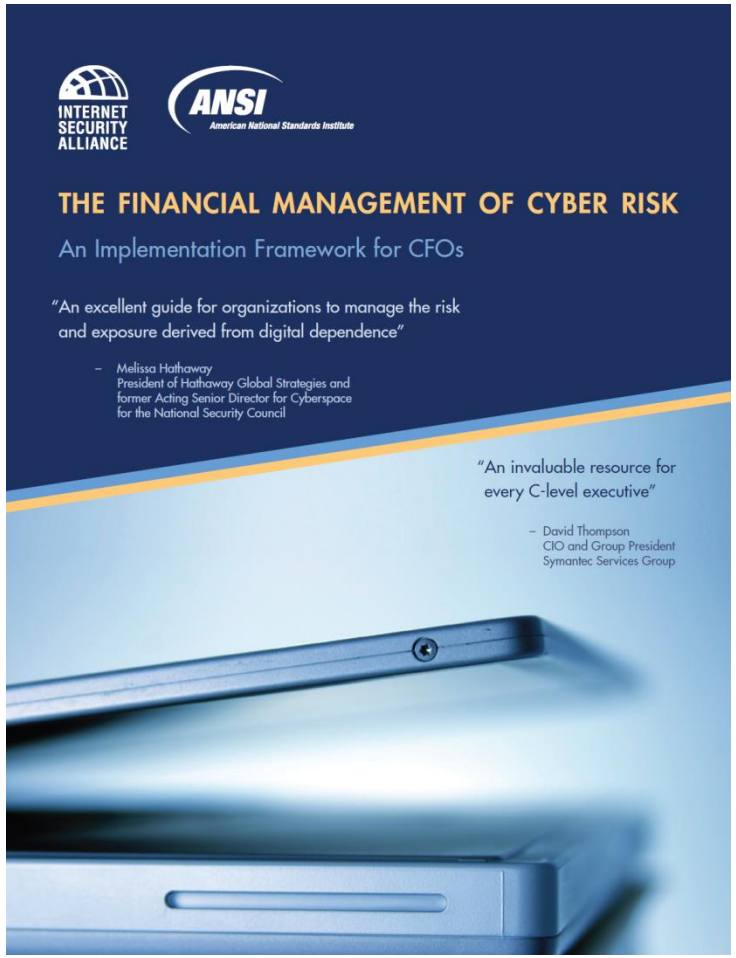
- Notable outcomes cited by survey respondents include identification of key risks, fostering an organizational culture of security and better alignment of cybersecurity with overall risk management and business goals. Perhaps more than anything, Board participation opened the lines of communication between the cybersecurity function and top executives and directors

  -- PWC 2016 Global Information Security Survey

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?)

Principle 4: Developing a Cyber Risk Management Framework



Principle 4: Knowledge & Skills for Cyber Risk Management

- Critical thinking
- Understanding of probability
- Training in calibrated estimation
- Comfort with numbers
- Familiarity decision methods
- Familiarity with the business
- Proper Cyber Risk Management uses a systematic, ideally empirical, enterprise wide risk assessment and management framework

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

Three Lines of Cyber Defense --- (3LoD)

- Line 1 – operates the business, owns the risk designs and implements operations
- Line 2 – defines policy statements & defines RM framework. Provides a credible challenge to the first line & responsible for evaluating risk exposure for board to determine risk appetite
- Line 3 – commonly internal audit responsible for independent evaluation of the first and second lines

The first line of defense

- Provide through exam—is the business doing enough? (not one size fits all). Each business line defines the cyber risk they face & weave cyber risk and self assessment into fraud, crisis management and resiliency process.
- Business lines need to actively monitor existing and future exposures, vuls threats and assess what impact cber risk has on new tech deployment, client relationships, and business strategies

The second line of defense

- Should be walled off as a separate independent function. Manages enterprise cyber risk appetite and RM framework within overall enterprise risk –challenges the first line. Determines how to appropriately measure cyber risk and integrates into a risk tolerance statement for the firm
- Focus of first and second tiers needs to be on effectively managing risk – not regulatory compliance – although can integrate compliance

Third Line of defense

- Provides independent objective assessment of firms process across lines one and two with focus on operational effectiveness and efficiency. Traditionally I audit relied on frameworks (NIST) but firms will likely need to develop their own to adapt to enhanced threats
- IA perform assessments validate tech infrastructure and third party risks, do independent Pen testing and must stay abreast of threat intel

Principle 5 Principle in Modern Cyber Risk Management

- Focus not on attacks but impacts
- Clear terms, better scoping, no bogus math
- Place cyber events in quantitative economic terms
- Prioritize cyber risk to the business
- Do you need to keep spending on this ____?
- Are these risks, really risks, or just innovations?
- A new – better – direction for Govt. and Industry -- See Hubbard, FAIR, X-Analytics Models

Principle 5: A Modern Risk Assessment – What to Accept, Reject Mitigate Transfer

- What exactly is your risk appetite?
- 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?
- Practice, practice practice

Market Advances in Cyber Risk Management

- Focus not on attacks but impacts
- Clear terms, better scoping, no bogus math
- Place cyber events in quantitative economic terms
- Prioritize cyber risk to the business
- Do you need to keep spending on this _____?
- Are these risks, really risks?
- The marketplace yields FAIR and X Analytics (AIG)
- A new – better – direction for Govt. and Industry

Basic Cyber Risk Assessment Economics Methodology

- Using best available data make probabilistic assessment of possible scenarios – looking for accuracy not precision
- Focus on scenarios that are probable and have enough expected loss to matter
- Calculate best case, worst case, most likely case and what degree of loss is acceptable (risk appetite)
- Determine investment required to mitigate to an acceptable level
- Option: run multiple scenarios (Monte Carlo simulations)

Title An Ultra Simple Example of Economic Risk Assessment

- Based on internal/external information how many events (e.g. DOSS) attacks will you experience?
- What percentage of these will be successful?
- What is the cost of this "successful" attack?
- Monte Carlo simulation to determine a arrange of loss events (minimum/most likely/average/max)
- Graph probability of loss vs. mitigation cost e.g. 65% chance of loss =x$ =worth of mitigation

Resolution