INTERNET SECURITY ALLIANCE

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

INTERNET SECURITY ALLIANCE

Problem

INTERNET SECURITY ALLIANCE

A BRIEF HISTORY OF

TECHNOLOGY USE AND

BANK CRIME

Then and Now

- 100 years ago Bonnie and Clyde used advanced technology (fast cars) and antiquated laws (drove across state lines) to successfully rob banks
- Dillinger: Why do you rob banks? Because it's easy
- Today sophisticated cyber criminals are using advanced technological methods and an antiquated law enforcement structure to rob banks ---- and everyone else

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.

INTERNET SECURITY ALLIANCE

Barriers

We don't understand the problem

- Hackers?
- Just Credit Cards and PII
- They Don't Care about me (70% at small business)
- Over confidence in the C-Suite (70% confident)
- Firewalls and passwords?
- Cyber Security is a defensive strategy
- If your thinking about **computer** security

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
- We don't have enough people

Financial Services Barriers to cyber security

- Third Party Vendors
- Complex Technology
- Nation State Attackers
- Lack of clear guidance from regulators
- Vulnerability across the enterprise

- Source PWC Global Info Security Survey 2017

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

Longing for Bonnie and Clyde and Johnny D

Richard Ledgett, Deputy Director National Security Agency said "Research has linked the Sony Pictures attack with the Bangladesh bank heist ($80 million) and affirmed that he believed that nation states are in the business of robbing banks." (NYT March 26 2017)

Criminals Are Just As Good (Bad)

"While nation states continue to set a high bar for sophisticated cyber attacks some financial threat actors have caught up to the point where we no longer see a line separating the two" FireEye M-Trend Reports March 2017

Lack of clear guidance

- Some firms are now spending 40% of CISO time on regulatory compliance
- Some firms are spending 30% of their cyber security budgets on compliance
- There are more than 60 separate security standards just for financial institutions
- 67 of the 73 topic categories in the Risk Compliance Management have redundant sources

Need to Change Your Security Model

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)

INTERNET SECURITY ALLIANCE

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

INTERNET SECURITY ALLIANCE

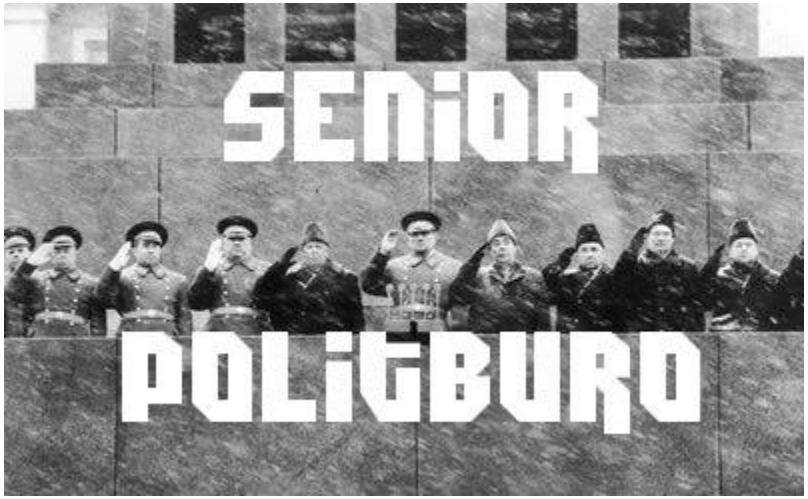
Champion

INTERNET SECURITY ALLIANCE

Government

INTERNET SECURITY ALLIANCE

Kremlinology



INTERNET SECURITY ALLIANCE

Trumpology

Lt. Gen. H.R. McMaster
National Security Advisor

General Keith Kellogg
National Security Council

Steven Bannon

Donald McGahn
General Counsel

Gen. James Mattis
Sec of Dep. of Defense

Mike Pence
Vice President

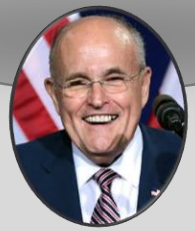
President Donald Trump

Tom Bossert
Homeland
Security Advisor

Gen. John Kelly (USMC – Ret.)
Sec of Dep. of Homeland Security

Josh Steinman

Karen Evans



Rudy Guiliani
Former Mayor of NYC

Steven Mnuchin
Sec. of Dep. of
Treasury

Adm. Mike Rogers
Director of National
Intelligence

ISA's Cybersecurity Social Contract

Copies of ISA's Cybersecurity Social Contract can be obtained online at Amazon.com.

ISA/NACD Cyber-Risk Oversight Handbook

Copies of the ISA/NACD Cyber-Risk Oversight Handbook can be obtained at:
http://www.isalliance.org/cyber-risk-handbook

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

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?)

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

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

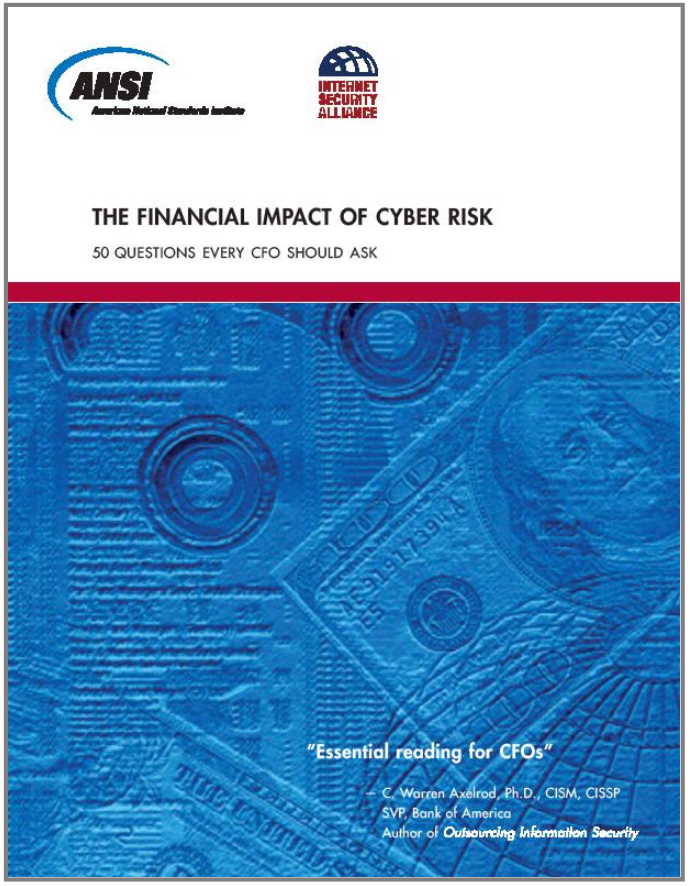
- Reputation Risk ---will anyone do business with you ---are you inviting regulatory scrutiny?

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

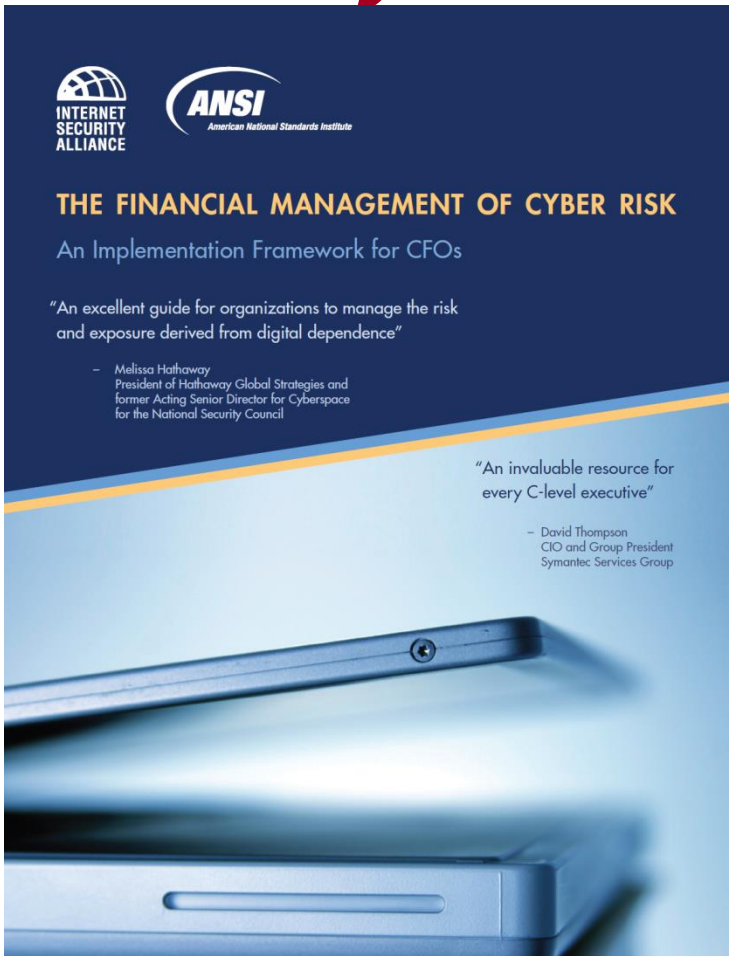
50 Questions Every CFO Should Ask

"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.



Financial Management of Cyber Risk



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

AICPA Re-thinking the cyber security audit process

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