How Risk Economics Can Help win the battle to Secure Cyberspace

Larry Clinton, President, ISA

FAIR22 CONFERENCE

ISA Mission and Goals

- ISA MISSION: To integrate advanced technology with economics and public policy to create a sustained system of cyber security.

- ISA GOALS
  - Develop thought leadership in cyber security
  - Advocate for enlightened public policy
  - Promote effective standards, practices and tech
  - Maintain ISA as viable, strong & effective

FAIR22 CONFERENCE

ISA Board of Directors 2022

Chairman

- JR Williamson, Sr., VP and Chief Information Security Officer, Leidos

First Vice Chair

- Tracie Grella, Global Head of Cyber Insurance, AIG

Second Vice Chair

- Lisa Humbert, Operational Risk Management Officer for the Americas, Union Bank

Immediate Past Chair

- Tim McKnight, Chief Information Security Officer, SAP SE

Directors

- Wil Bennett, VP Chief Information Security Officer, USAA
- Shaun McAdams, Director - Cyber Threat Operations, Raytheon Technologies
- Dimitrios Stratakis, Director, Chief Technology Risk Officer, BNY Mellon
- Richard Spearman, Group Corporate Security Director, Vodafone
- Andrew Cotton, Partner, Assurance Services, Ernst and Young
- Tim McNulty, Cylab Associate Vice President of Government Relations, Carnegie Mellon University

FAIR22 CONFERENCE

ISA Board of Directors 2022

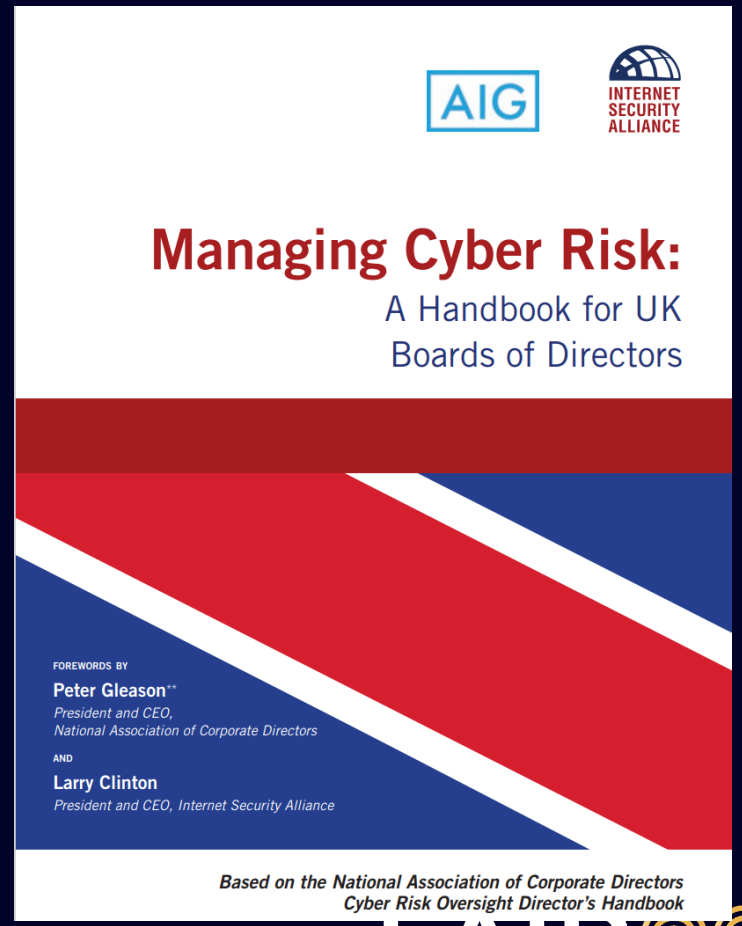
- Robert Vescio, Inventor, X-Analytics
- John Frazzini, President and CEO, Secure Systems Innovation Corporation & X-Analytics
- Deneen DeFiore, VP & Chief Information Security Officer, United Airlines
- Ted Webster, VP, Security Governance, Risk and Compliance, Centene
- Robyn Boerstling, Vice President, Infrastructure, Innovation and Human Resources Policy, NAM
- Richard Rocca, Chief Information Security Officer, Bunge Limited
- Greg Montana, CEVP, Chief Risk Officer, FIS
- Ryan Boulais, Chief Information Security Officer, AES Corp
- Michael Woods, CISO, GE
- Andy Kirkland, CISO Global Cyber Security, Starbucks
- Michael Higgins, VP, Information Security & CISO, L3 Harris
- Jon Brickey, SVP, Cybersecurity Evangelist, Mastercard
- Carolann Shields, Chief Information Security Officer, Baker Hughes
- Nick Sanna, CEO, RiskLens
- Larry Clinton, President and Chief Executive Officer, Internet Security Alliance

FAIR22 CONFERENCE

OAS version

Pan-European version

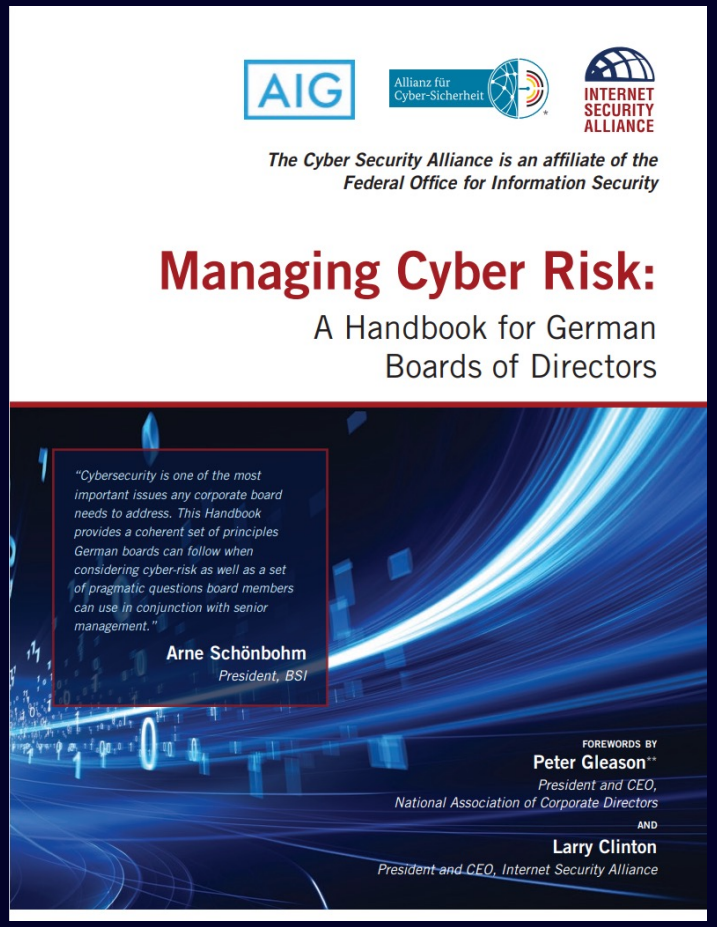
UK version



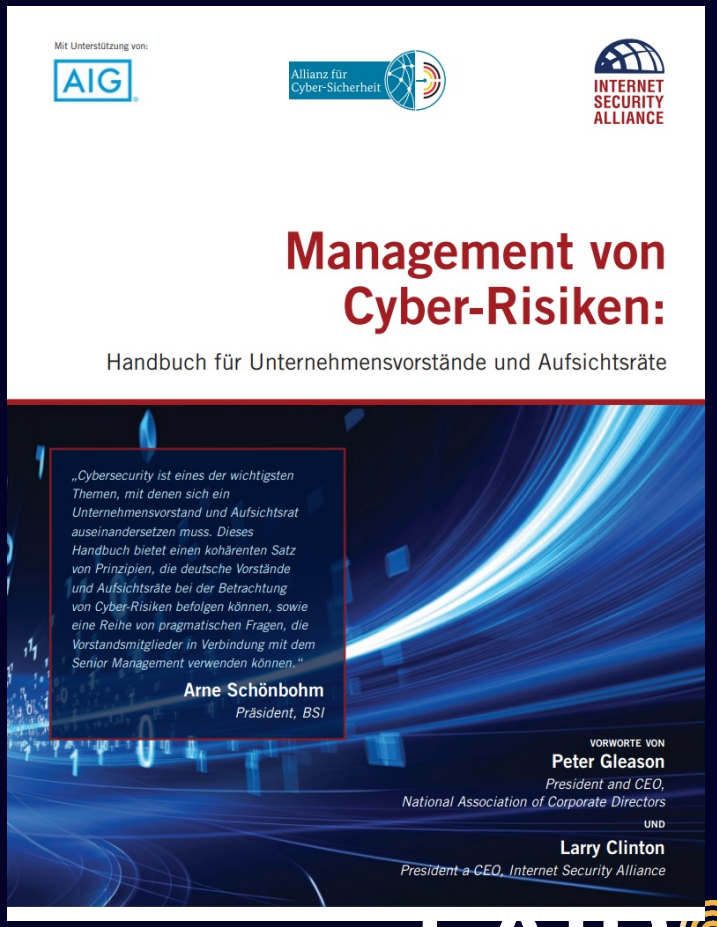
FAIR 22 CONFERENCE

Japanese version

German version in English

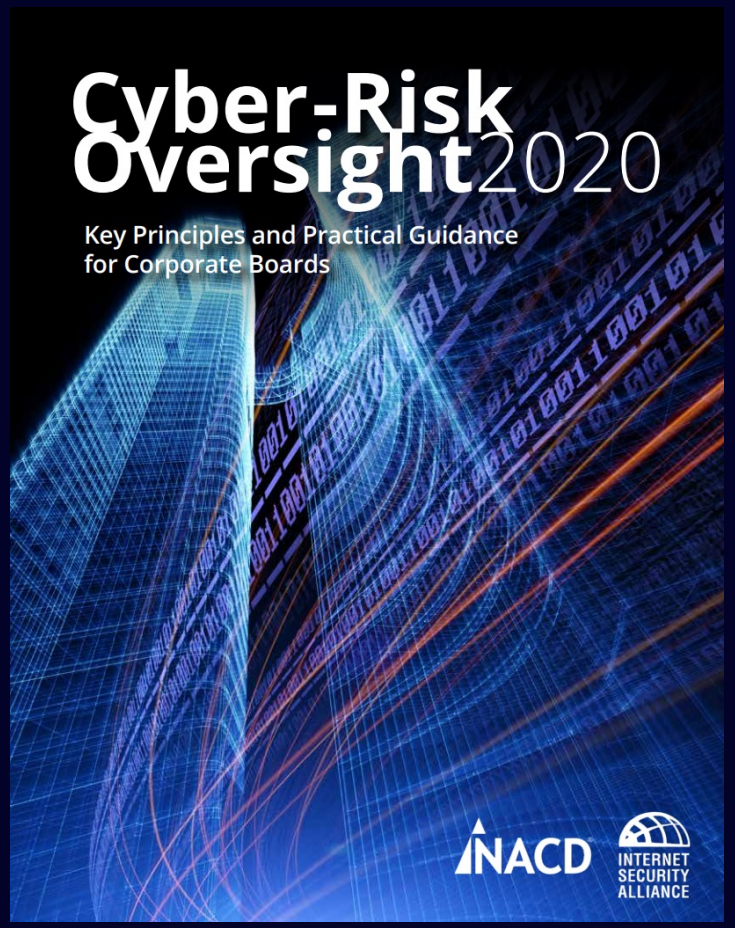


German version in German

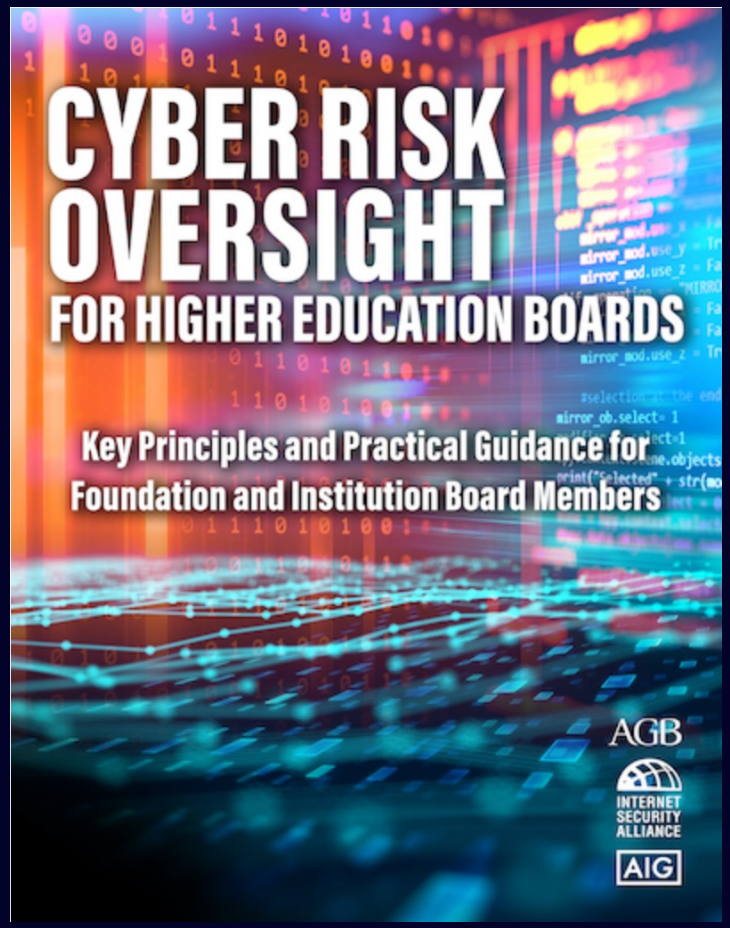


FAIR'22 CONFERENCE

NACD Cyber-Risk Oversight 2020

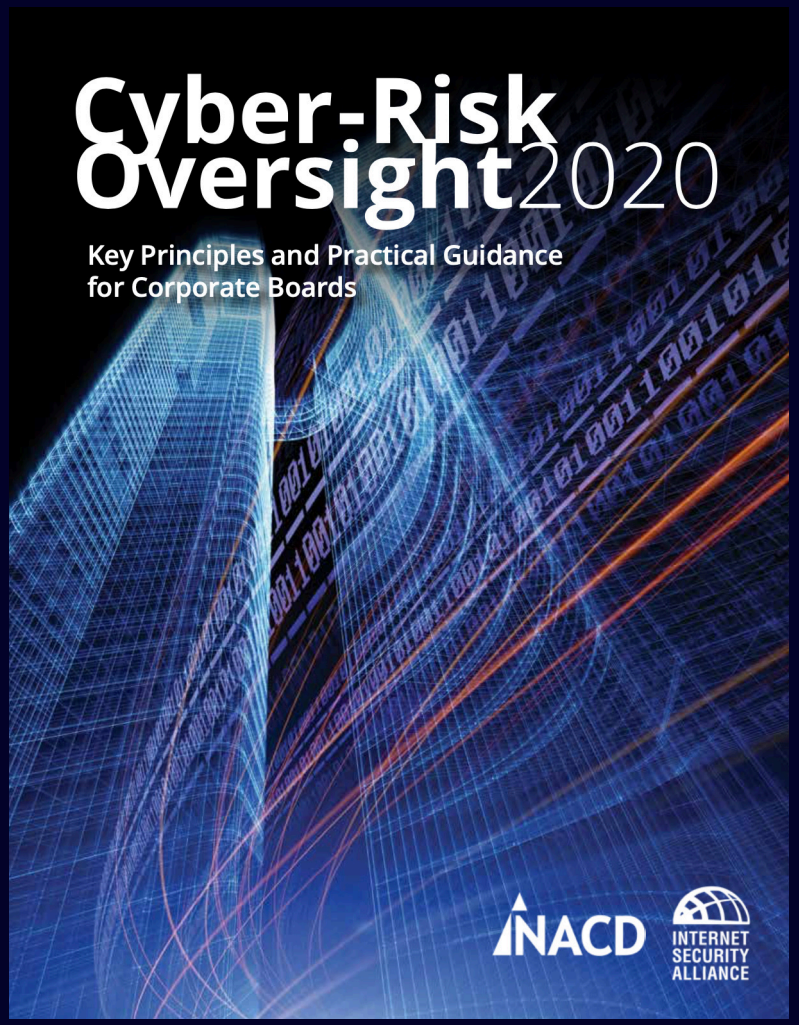


AGB Handbook for College/ University Boards



Asia-Pacific Version

NACD – ISA cyber principles



- Cyber is a strategic, enterprise-wide issue, not an IT issue
- Boards need to understand their unique legal obligations
- Boards need to access adequate cyber security expertise
- Management needs to provide a cyber security framework (technical and management)
- Management must do risk assessment

Industry Support for NACD-ISA Handbooks on Cyber Risk

- National Association of Corporate Directors
- Internet Security Alliance
- Center for Audit Quality
- European Conference of Directors Associations
- Cyber Security Council of Germany
- Japanese Federation of Businesses
- Association of Indian Telecommunications and Infrastructure
- FAIR

Gov. Support for the NACD- ISA Cyber Risk Handbooks

- US Department of Homeland Security
- US Department of Justice
- German Federal Office of Information Security (BSI)
- Organization of American States

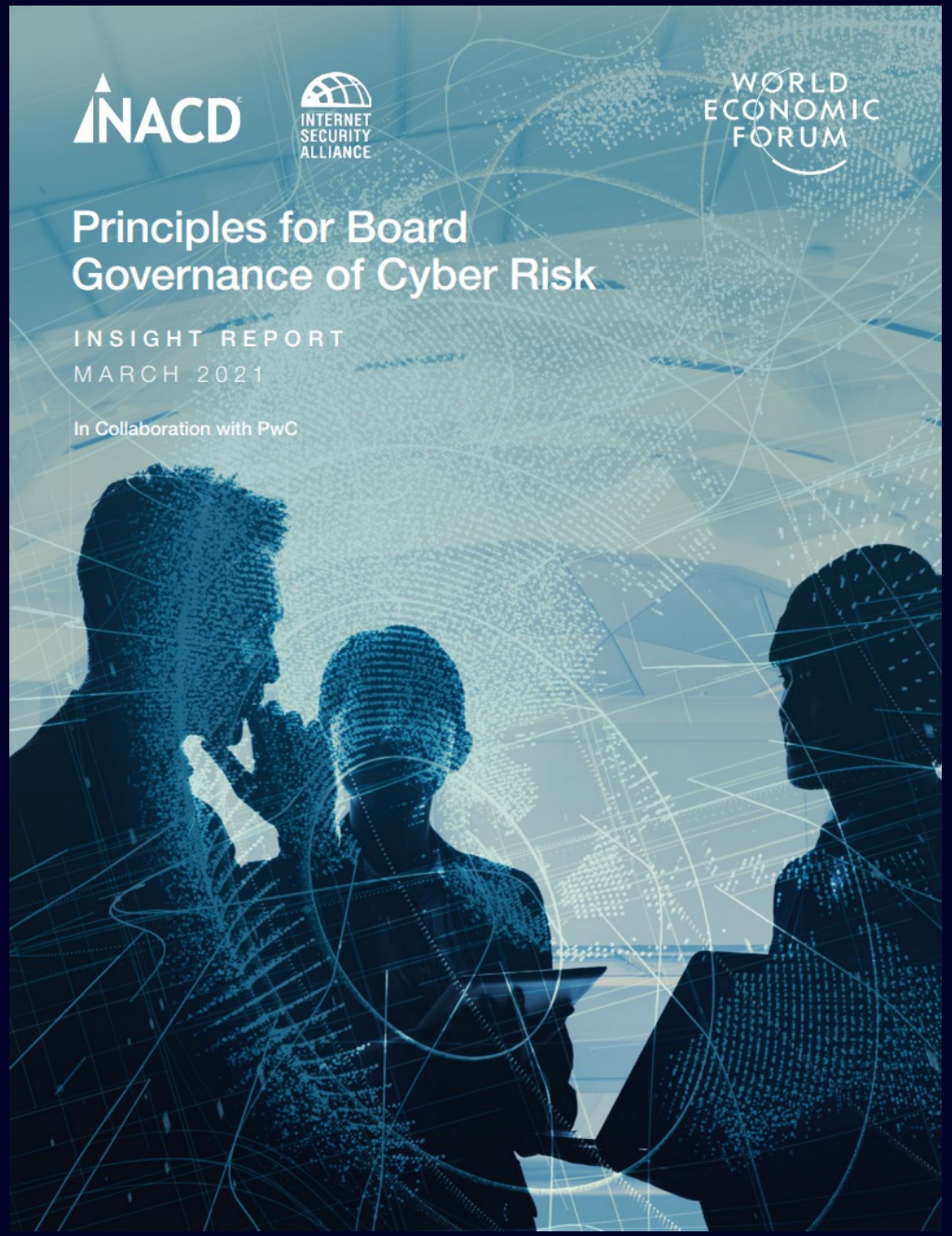
PwC on Effectiveness of NACD Handbook

"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 cyber security 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 cyber security practices in numerous ways. It may be no coincidence that, as more Boards participate in cyber security budget discussions, we saw a 24% boost in security spending."

PwC on Effectiveness 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. More than anything, board participation has opened the lines of communication between executives and directors treating cyber security as an economic issue."



NACD

ISA

World Economic Forum

FAIR22 CONFERENCE

The WEF/ISA CEO Cyber Pledge

- Joint Effort for World Economic Forum, National Association of Corporate Directors and ISA to expand acceptance of the 6 consensus core principles both world-wide and including senior management.

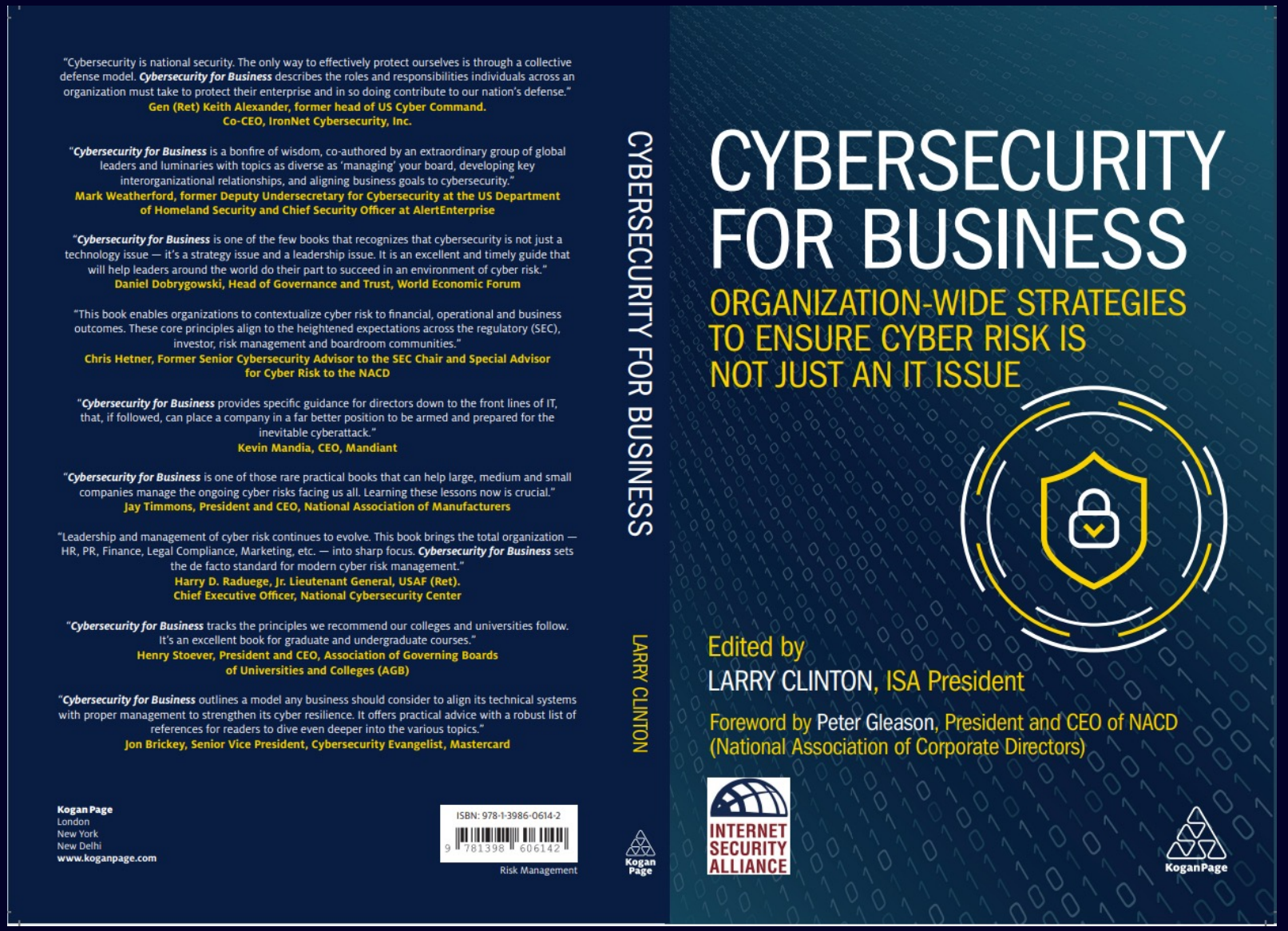
- Seeking CEO support to implement core principles and commitment to urge their peers to also expand collaborartiton

Principles for board governance of cyber risk

Cyber-Risk Principles

1. Cybersecurity is a strategic business enabler
2. Understand the economic drivers and impact of cyber risk
3. Align cyber-risk management with business needs
4. Ensure organizational design supports cybersecurity
5. Incorporate cybersecurity expertise into board governance
6. Encourage systemic resilience and collaboration

Cybersecurity for Business



"Cybersecurity is national security. The only way to effectively protect ourselves is through a collective defense model. ***Cybersecurity for Business*** describes the roles and responsibilities individuals across an organization must take to protect their enterprise and in so doing contribute to our nation's defense."
Gen (Ret) Keith Alexander, former head of US Cyber Command.
Co-CEO, IronNet Cybersecurity, Inc.

"***Cybersecurity for Business*** is a bonfire of wisdom, co-authored by an extraordinary group of global leaders and luminaries with topics as diverse as 'managing' your board, developing key interorganizational relationships, and aligning business goals to cybersecurity."
Mark Weatherford, former Deputy Undersecretary for Cybersecurity at the US Department of Homeland Security and Chief Security Officer at AlertEnterprise

"***Cybersecurity for Business*** is one of the few books that recognizes that cybersecurity is not just a technology issue — it's a strategy issue and a leadership issue. It is an excellent and timely guide that will help leaders around the world do their part to succeed in an environment of cyber risk."
Daniel Dobrygowski, Head of Governance and Trust, World Economic Forum

"This book enables organizations to contextualize cyber risk to financial, operational and business outcomes. These core principles align to the heightened expectations across the regulatory (SEC), investor, risk management and boardroom communities."
Chris Hetner, Former Senior Cybersecurity Advisor to the SEC Chair and Special Advisor for Cyber Risk to the NACD

"***Cybersecurity for Business*** provides specific guidance for directors down to the front lines of IT, that, if followed, can place a company in a far better position to be armed and prepared for the inevitable cyberattack."
Kevin Mandia, CEO, Mandiant

"***Cybersecurity for Business*** is one of those rare practical books that can help large, medium and small companies manage the ongoing cyber risks facing us all. Learning these lessons now is crucial."
Jay Timmons, President and CEO, National Association of Manufacturers

"Leadership and management of cyber risk continues to evolve. This book brings the total organization — HR, PR, Finance, Legal Compliance, Marketing, etc. — into sharp focus. ***Cybersecurity for Business*** sets the de facto standard for modern cyber risk management."
Harry D. Raduege, Jr. Lieutenant General, USAF (Ret).
Chief Executive Officer, National Cybersecurity Center

"***Cybersecurity for Business*** tracks the principles we recommend our colleges and universities follow. It's an excellent book for graduate and undergraduate courses."
Henry Stoever, President and CEO, Association of Governing Boards of Universities and Colleges (AGB)

"***Cybersecurity for Business*** outlines a model any business should consider to align its technical systems with proper management to strengthen its cyber resilience. It offers practical advice with a robust list of references for readers to dive even deeper into the various topics."
Jon Brickey, Senior Vice President, Cybersecurity Evangelist, Mastercard

Kogan Page
London
New York
New Delhi
www.koganpage.com

ISBN: 978-1-3986-0614-2

Risk Management

CYBERSECURITY FOR BUSINESS

LARRY CLINTON

CYBERSECURITY FOR BUSINESS

ORGANIZATION-WIDE STRATEGIES TO ENSURE CYBER RISK IS NOT JUST AN IT ISSUE

Edited by
LARRY CLINTON, ISA President

Foreword by Peter Gleason, President and CEO of NACD (National Association of Corporate Directors)

INTERNET SECURITY ALLIANCE

KoganPage

FAIR22 CONFERENCE

Cybersecurity for Business

Chapter 1- Cybersecurity is (Not) an IT Issue

Chapter 2 - The View from the Top Cybersecurity and Boards of Directors

Chapter 3 - Structuring for the Digital Age

Chapter 4 - A Modern Approach to Assessing Cyber Risk

Chapter 5 - The Role of HR Functions in Scaling Cybersecurity and Building Trust

Chapter 6 - Cybersecurity and the Office of the General Counsel

Chapter 7 - Cybersecurity Audit and Compliance Considerations

Chapter 8 - Cyber Supply Chain and Third-party Risk Management

Chapter 9 - Technical Operations

Chapter 10 - Crisis Management

Chapter 11 - Cybersecurity Considerations During M&A Phases

Chapter 12 - Developing Relationships with the Cybersecurity Team

FAIR22 CONFERENCE

How much risk is there?

A little | None | A lot

Fixing American Cybersecurity

FAIR22 CONFERENCE

Clarke and Knake The Fifth Domain

- “Since the Clinton Administration our cybersecurity strategy has changed very little…companies that own and operate the internet will be responsible for protecting themselves. Government’s role will be limited to support the private victims of cyber-attacks with law enforcement, information sharing, diplomacy and in the rare cases military force.

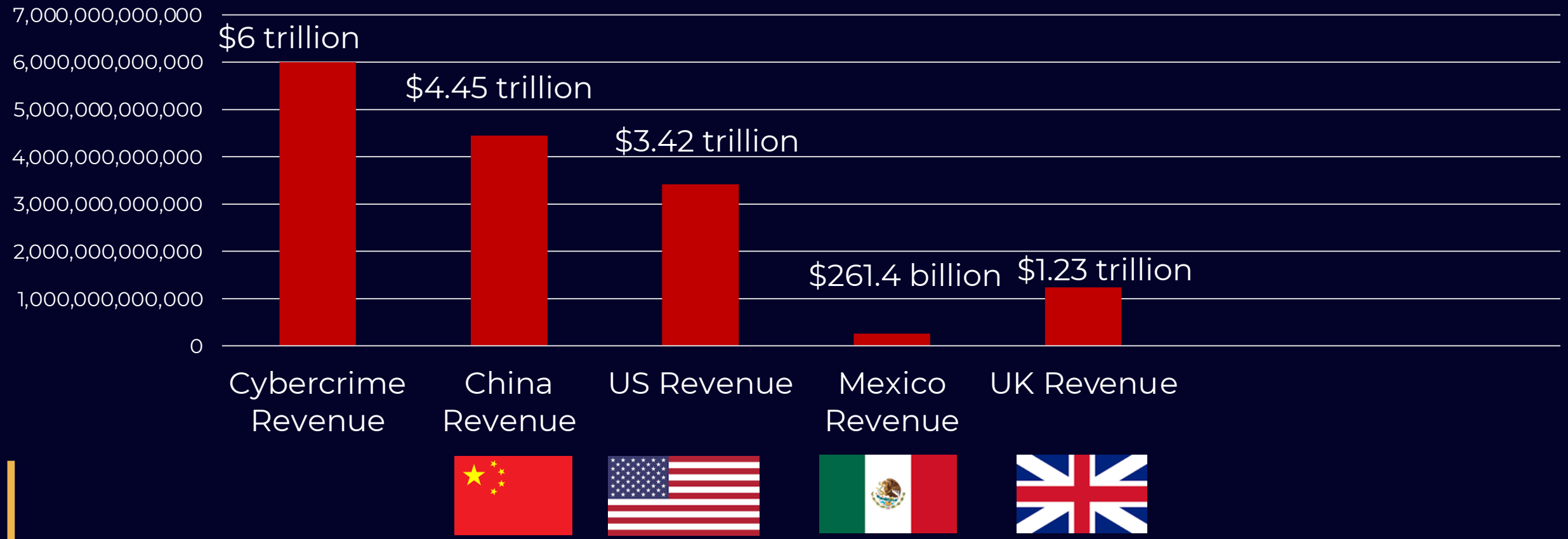
Clarke and Knake The Fifth Domain

Government also help industry help itself through nudges to encourage investment and cooperation in cybersecurity through research training convening and ultimately through regulation.”

How Bad is it? Really Bad

- Cyber Crime costs 2.2 Trillion a year (Equiv of Mexico)– rising to 10.5 T by 2025 Equiv of China
- DNI reports Cyber attacks are a larger threat to USA than international terrorism
- Nation States regularly and successfully attack the USA – OPM, 2016/18 Elections Solar Winds

Cybercrime revenue vs. nation-state revenues



Marcus Aurelius

“Of All Things Ask What is their Essence!”

We Are Not Asking the Right Questions

- Overwhelming focus of cyber policy has been on the technology – the HOW of Cyber Attacks
- To solve the problem need to address Economics – the WHY of cyber attacks
- Verizon 86% of cyber attacks are economically motivated
- Analyzing technology with out considering economics is as misguided as analyzing economics without considering technology

Is Our Infrastructure Vulnerable? YES!
Is that the Essence of the Problem? NO.

- The Internet was built vulnerable – it's an open system
- The system is getting technically more vulnerable all the time --- technology VOIP/Cloud/mobile devices
- The business practices create new vulnerabilities – BOYD/long international supply chains/web-based marketing and remote employees
- Avg # of malicious code Microsoft discovers every month 77,000
- # of Patches Oracle applied to its cloud in 2018 – 150,000,000
- But Cyber is not alone – water/food/transport also vulnerable

Anderson and Moore's Economics of Information Security

"Security failure is caused as least as often by bad economic incentives as by bad technological design. 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."

Cost of Entry for Cyber Crime is Low

Go on the Dark Web and …

- You can “buy”(outsource) a DOS attack for apx $500
- You can “buy” access to corp. mail boxes for apx $200
- You can “buy” fake Instagram/Twitter addresses for apx $100
- Tutorial on how to conduct email attacks -- $25
- Purchase a Template to conduct the attack -- $3
- Creating a “dummy” retail website -- $24.43 – creating a dummy banking website -- $67.91

Cyber Criminals Invest in the business

"Cybercriminals at the high end are as technologically sophisticated as the most advanced IT companies and like them have moved quickly to adopt cloud computing, artificial intelligence, and encryption."

Bottom Line on Cyber Crime

- McAfee 2018 Cyber Crime Report

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

WE Need to Understand cyber from an Economics Point of View – like FAIR/NACD

- Cyber is NOT just a technical issue (P1 NACD-ISA)
- We Need to Understand our Obligations (P2)
- We Need to Access Adequate Cyber Expertise (P3)
- We Need to do Sophisticated Cybersecurity Risk Assessments – Empirical and Economics based (P4)
- Need a Clear Strategy – Govt Digital Transformation (P5)
- We Need to Work Together – beyond our boundaries (P6)

Example 1: Cyber Workforce Development

- Its really National Defense Mobilization
- What is the Essence of the Problem? Tech or Economics
- Is this like World War II ? Yes
- To Solve an Economic (cyber) problem you use Market incentives – A National, virtual, Cybersecurity Academy
- In Needs to be done at SCALE – 10,000 a year
- A National Academy could SOLVE the federal workforce problem in 4 years and do more….

Academy Status

- Endorsed by ISA and Association of Governing Boards
- “Starter Language” in both House and Senate versions of the National Defense Authorization Act (Gillibrand and Houlihan/Garbarino/Gallagher)
- Needs to be Expanded on Senate floor and then get appropriations

FAIR22 CONFERENCE

Example Two: Protecting Critical Infrastructure (P3)

- Digitization Makes Critical Infrastructure More Vulnerable than Ever
- What is the Essence of the Issue ? Private Entities having to finance security at a national security level
- Industry and government assess risk on legitimately different basis (current National Infrastructure Plan)
- Some in Gov say just put it on the shareholder – that's not sustainable – we actually need shareholders
- WE need a new system of economic incentives

Example Two: Protecting Critical Infrastructure (P3)

- Three criteria for incentives: 1) Need to be relevant to the industry 2) Need to have a “strike zone” what qualifies getting the incentive 3) Needs to be powerful enough to impact behavior
- We need to consider the government’s economics also
- Taxes – just for small companies, but other things are liability, regulatory relief, zoning privileges, procurement advantages, insurance (insurance companies have economics too) – we need to be creative

Example 3: Regulatory Reform (P 4& 5)

- What is the essence of the problem?
- The regulatory model (from the 19th century) is a poor fit for the digital age.
- Regulation is a slow, unproven, backward looking, wasteful, check the box mostly one-size fits all exercise
- Cybersecurity is a fast moving, forward looking risk management issue that needs to be empirically tied to the core to business plan/strategy
- Traditional regulation doesn't work e.g. Healthcare – but other regulated sectors also.

Example 3: Regulatory Reform (P 4 & 5)

- If you are going to mandate anything, why not mandate (or incentivize) entities to to a sophisticated cyber risk assessment and tie cyber funding to an empirical level based on the business plan.
- If that commercial level security is not adequate for national security purposes – then we need market incentives.
- Government needs to put whatever it does on an empirical, cost effective basis – start with NIST

Going Beyond our Borders – Scale --(P 6)

- Going where no one has gone before.
- We need a sustainable, egalitarian public private partnership
- Not a parent child relationship, more like a good marriage
- It has been done before – NASA, SEMATECH Operation Warp Speed, New CHIPS legislation
- Is it fair to ask the FAIR Institute and its members to help lead?

Kirk Piloting the *Kelvin* on a collision course

"Kirk Piloting the *Kelvin* on a collision course," George Kirk (alternate reality). *Memory Alpha*. Paramount Pictures. Retrieved from https://static.wikia.nocookie.net/memoryalpha/images/8/87/George_Kirk_commands_the_Kelvin.jpg/revision/latest?cb=20150912230158&path-prefix=en

FAIR22 CONFERENCE