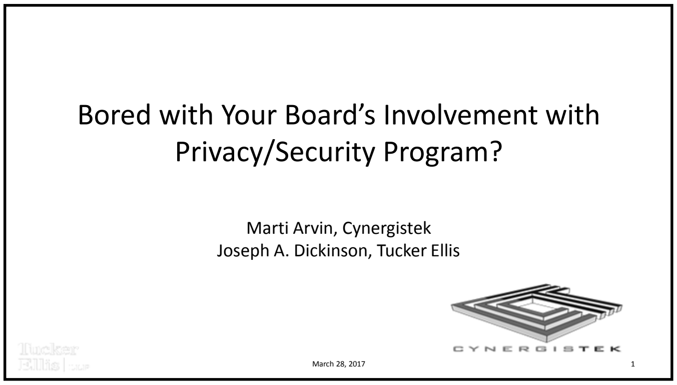


Bored with Your Board's Involvement with Privacy/Security Program?

Marti Arvin, Cynergistek
Joseph A. Dickinson, Tucker Ellis

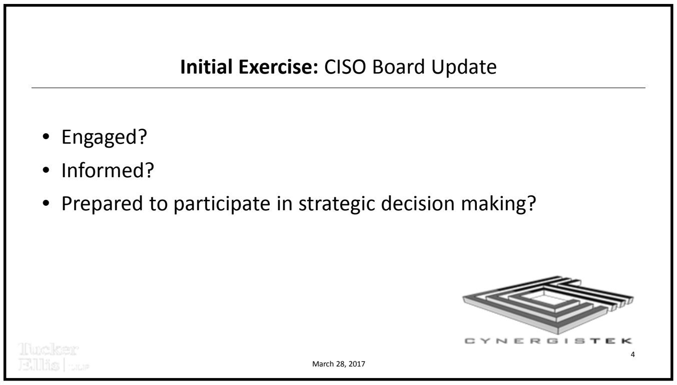
March 28, 2017 1

Initial Exercise: CISO Board Update

- Board of Directors/Trustees Monthly Security Program Update

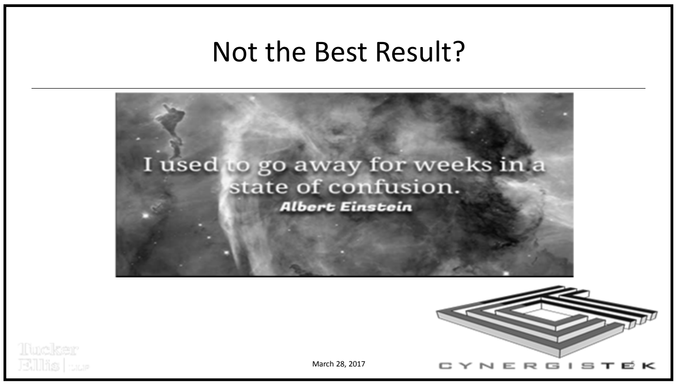
March 28, 2017 2

March 28, 2017 3



Initial Exercise: CISO Board Update

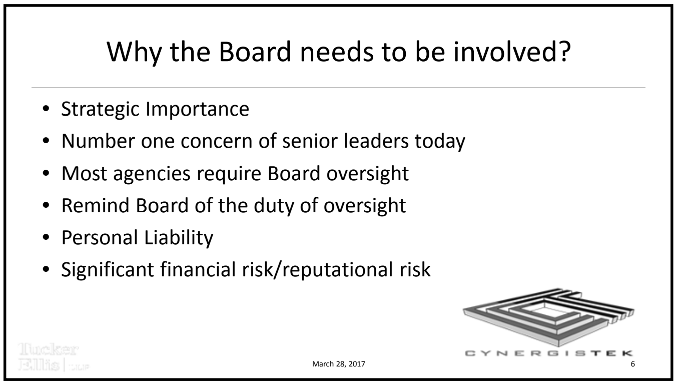
- Engaged?
- Informed?
- Prepared to participate in strategic decision making?



Not the Best Result?

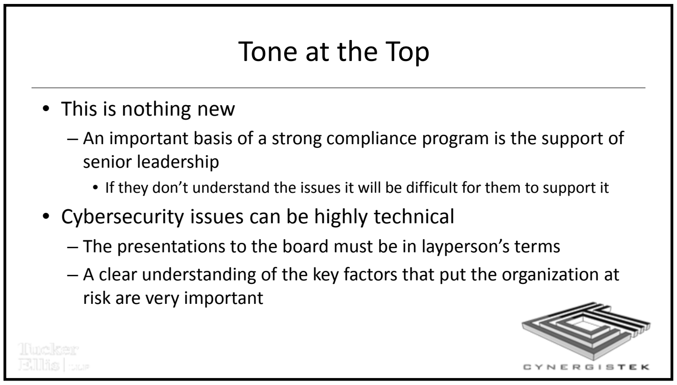
I used to go away for weeks in a state of confusion.

Albert Einstein



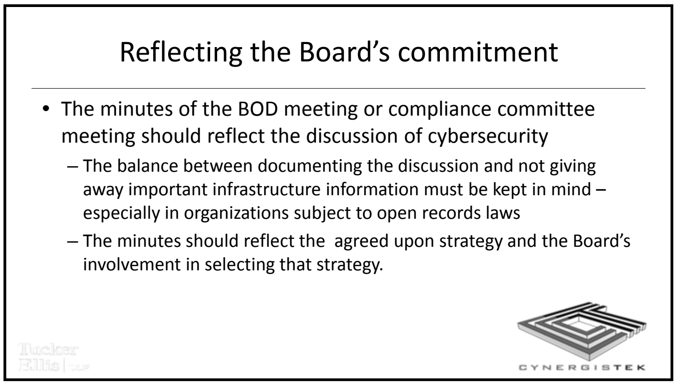
Why the Board needs to be involved?

- Strategic Importance
- Number one concern of senior leaders today
- Most agencies require Board oversight
- Remind Board of the duty of oversight
- Personal Liability
- Significant financial risk/reputational risk



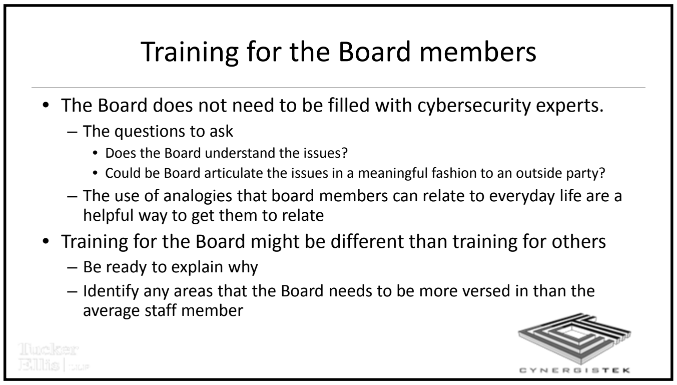
Tone at the Top

- This is nothing new
  - An important basis of a strong compliance program is the support of senior leadership
    - If they don't understand the issues it will be difficult for them to support it
- Cybersecurity issues can be highly technical
  - The presentations to the board must be in layperson's terms
  - A clear understanding of the key factors that put the organization at risk are very important



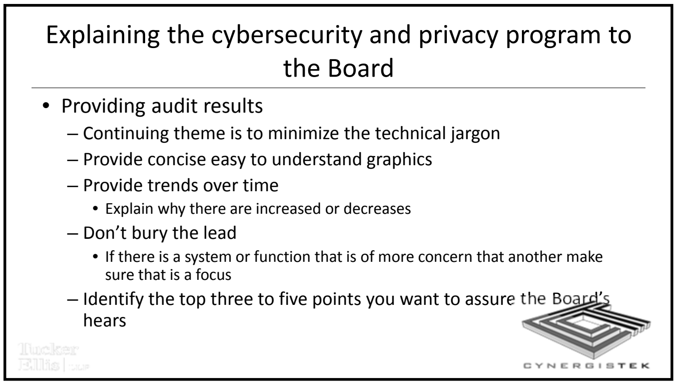
Reflecting the Board's commitment

- The minutes of the BOD meeting or compliance committee meeting should reflect the discussion of cybersecurity
  - The balance between documenting the discussion and not giving away important infrastructure information must be kept in mind – especially in organizations subject to open records laws
  - The minutes should reflect the agreed upon strategy and the Board's involvement in selecting that strategy.



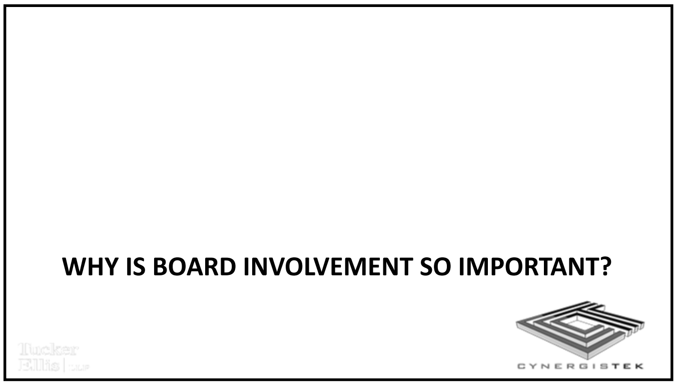
Training for the Board members

- The Board does not need to be filled with cybersecurity experts.
  - The questions to ask
    - Does the Board understand the issues?
    - Could be Board articulate the issues in a meaningful fashion to an outside party?
  - The use of analogies that board members can relate to everyday life are a helpful way to get them to relate
- Training for the Board might be different than training for others
  - Be ready to explain why
  - Identify any areas that the Board needs to be more versed in than the average staff member

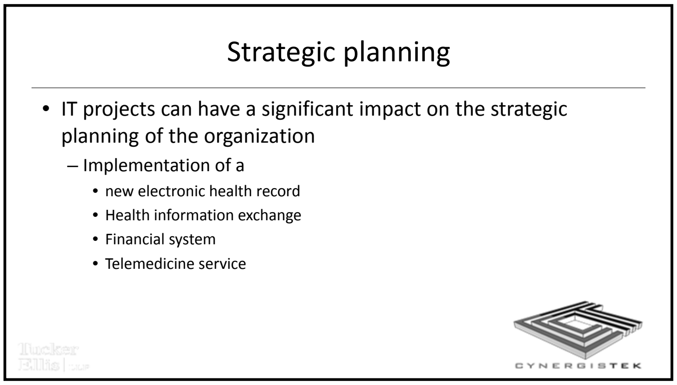


Explaining the cybersecurity and privacy program to the Board

- Providing audit results
  - Continuing theme is to minimize the technical jargon
  - Provide concise easy to understand graphics
  - Provide trends over time
    - Explain why there are increased or decreases
  - Don't bury the lead
    - If there is a system or function that is of more concern that another make sure that is a focus
  - Identify the top three to five points you want to assure the Board's hears

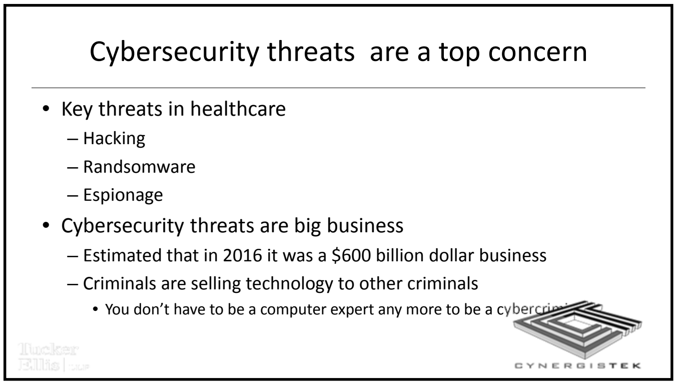


WHY IS BOARD INVOLVEMENT SO IMPORTANT?



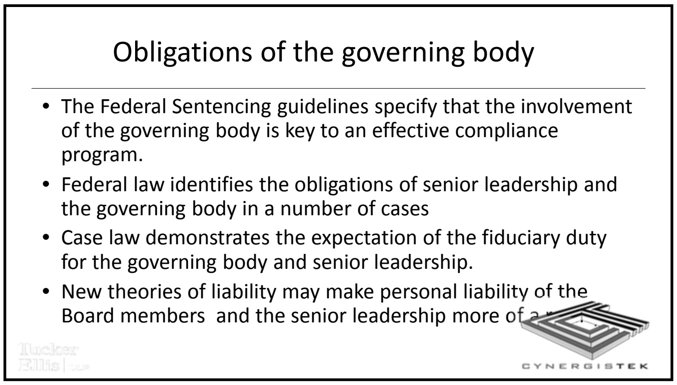
Strategic planning

- IT projects can have a significant impact on the strategic planning of the organization
  - Implementation of a
    - new electronic health record
    - Health information exchange
    - Financial system
    - Telemedicine service



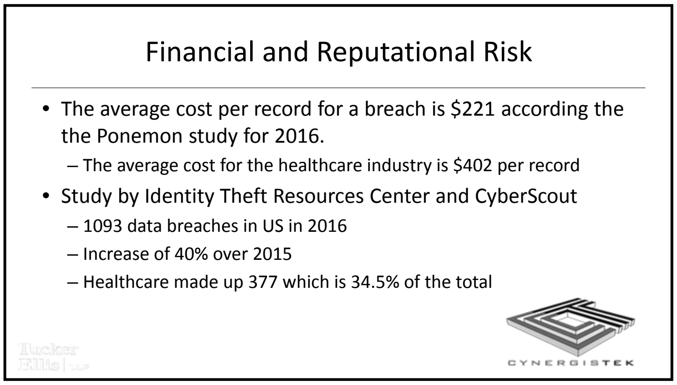
Cybersecurity threats are a top concern

- Key threats in healthcare
  - – Hacking
  - – Randsomware
  - – Espionage
- Cybersecurity threats are big business
  - – Estimated that in 2016 it was a $600 billion dollar business
  - – Criminals are selling technology to other criminals
    - You don't have to be a computer expert any more to be a cybercrimi



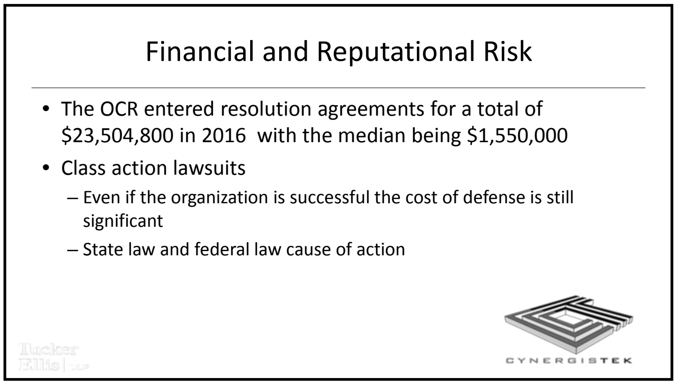
Obligations of the governing body

- The Federal Sentencing guidelines specify that the involvement of the governing body is key to an effective compliance program.
- Federal law identifies the obligations of senior leadership and the governing body in a number of cases
- Case law demonstrates the expectation of the fiduciary duty for the governing body and senior leadership.
- New theories of liability may make personal liability of the Board members and the senior leadership more of a



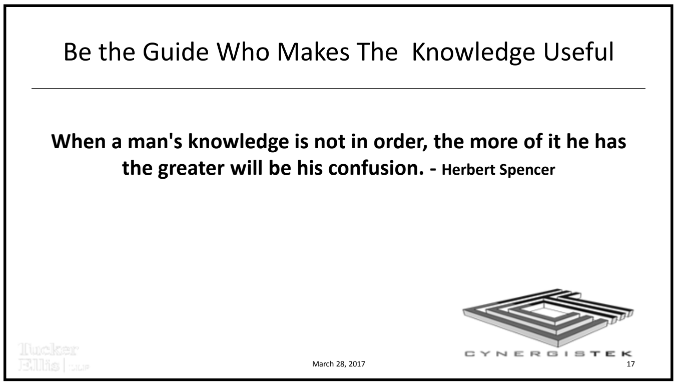
Financial and Reputational Risk

- The average cost per record for a breach is $221 according the the Ponemon study for 2016.
  - – The average cost for the healthcare industry is $402 per record
- Study by Identity Theft Resources Center and CyberScout
  - – 1093 data breaches in US in 2016
  - – Increase of 40% over 2015
  - – Healthcare made up 377 which is 34.5% of the total



Financial and Reputational Risk

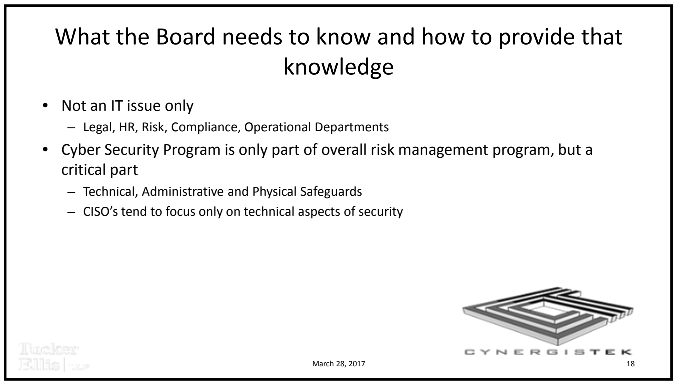
- The OCR entered resolution agreements for a total of $23,504,800 in 2016 with the median being $1,550,000
- Class action lawsuits
  - Even if the organization is successful the cost of defense is still significant
  - State law and federal law cause of action



Be the Guide Who Makes The Knowledge Useful

When a man's knowledge is not in order, the more of it he has the greater will be his confusion. - Herbert Spencer

March 28, 2017 17



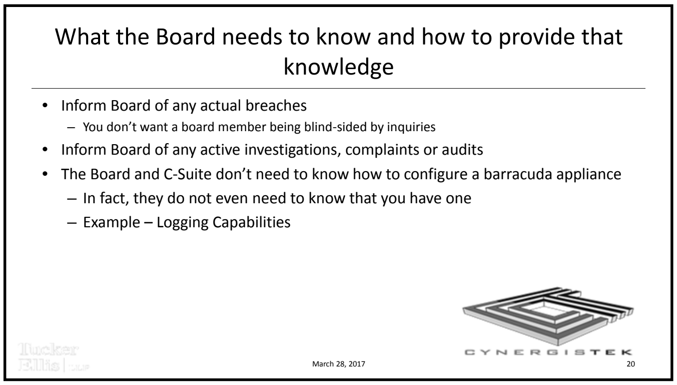
What the Board needs to know and how to provide that knowledge

- Not an IT issue only
  - Legal, HR, Risk, Compliance, Operational Departments
- Cyber Security Program is only part of overall risk management program, but a critical part
  - Technical, Administrative and Physical Safeguards
  - CISO’s tend to focus only on technical aspects of security

March 28, 2017 18

IT TURNS OUT THAT THE PEOPLE'S BIGGEST FEAR ABOUT CLOUD COMPUTING ISN'T 'DATA SECURITY', IT'S 'WHAT HAPPENS IF THERE'S A THUNDERSTORM?'
© D.Fletcher for CloudTweaks.com
Tucker Ellis LLP
CYNERGISTEK

March 28, 2017 19



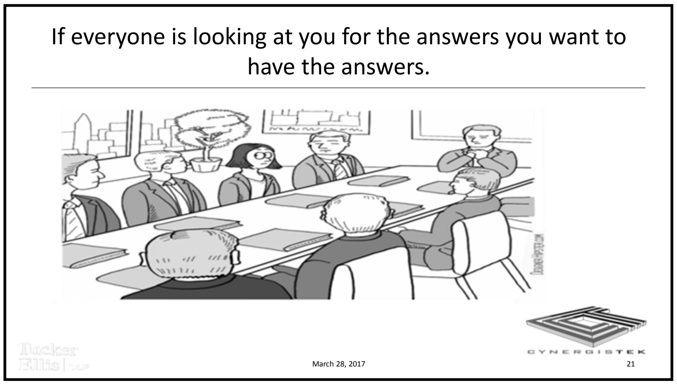
What the Board needs to know and how to provide that knowledge

- Inform Board of any actual breaches
  - You don't want a board member being blind-sided by inquiries
- Inform Board of any active investigations, complaints or audits
- The Board and C-Suite don't need to know how to configure a barracuda appliance
  - In fact, they do not even need to know that you have one
  - Example – Logging Capabilities

Tucker Ellis LLP

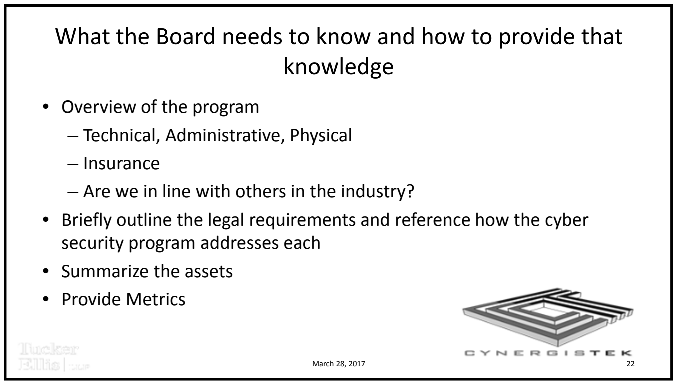
CYNERGISTEK

March 28, 2017 20



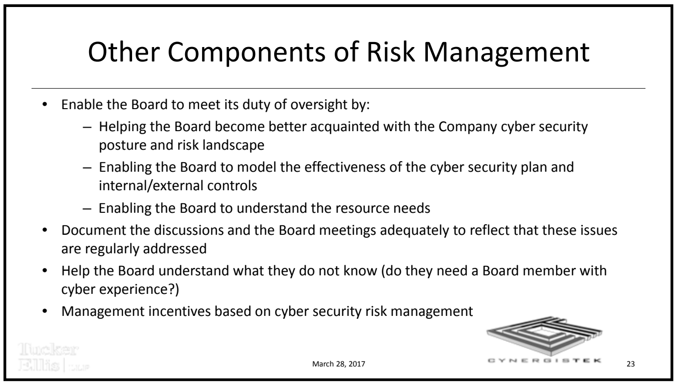
If everyone is looking at you for the answers you want to have the answers.

March 28, 2017 21



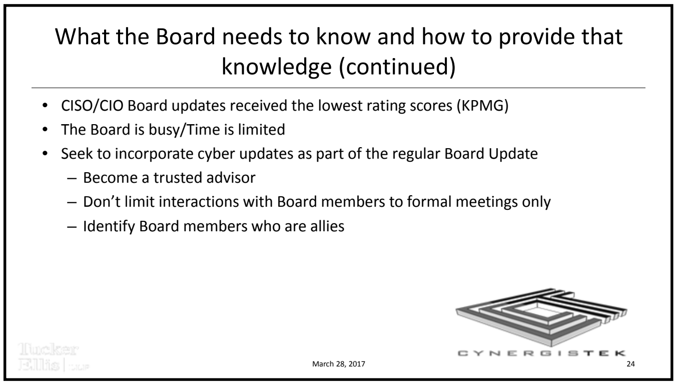
What the Board needs to know and how to provide that knowledge

- Overview of the program
  - Technical, Administrative, Physical
  - Insurance
  - Are we in line with others in the industry?
- Briefly outline the legal requirements and reference how the cyber security program addresses each
- Summarize the assets
- Provide Metrics



Other Components of Risk Management

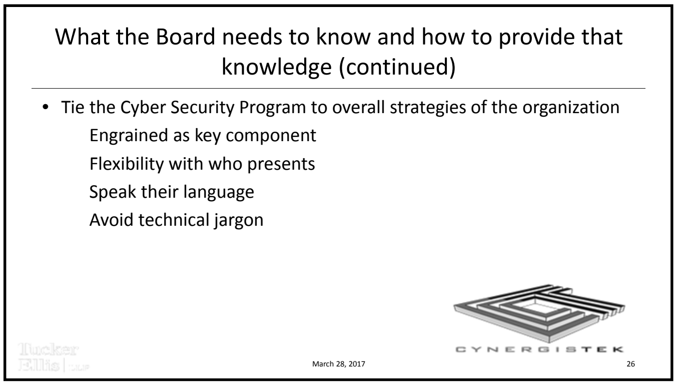
- Enable the Board to meet its duty of oversight by:
  - Helping the Board become better acquainted with the Company cyber security posture and risk landscape
  - Enabling the Board to model the effectiveness of the cyber security plan and internal/external controls
  - Enabling the Board to understand the resource needs
- Document the discussions and the Board meetings adequately to reflect that these issues are regularly addressed
- Help the Board understand what they do not know (do they need a Board member with cyber experience?)
- Management incentives based on cyber security risk management



What the Board needs to know and how to provide that knowledge (continued)

- CISO/CIO Board updates received the lowest rating scores (KPMG)
- The Board is busy/Time is limited
- Seek to incorporate cyber updates as part of the regular Board Update
  - Become a trusted advisor
  - Don't limit interactions with Board members to formal meetings only
  - Identify Board members who are allies

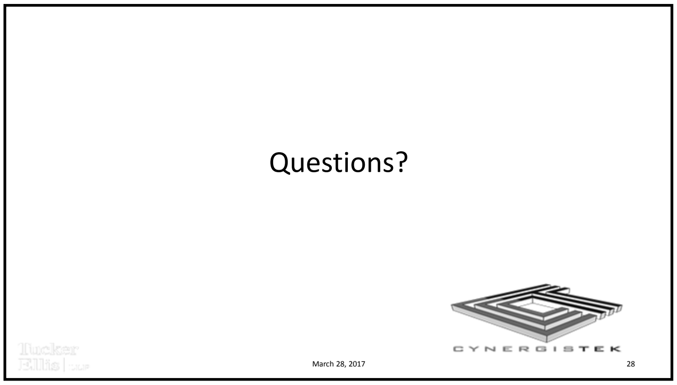
"To put it simply, our policy just isn't complicated enough."



What the Board needs to know and how to provide that knowledge (continued)

- Tie the Cyber Security Program to overall strategies of the organization
  - Engrained as key component
  - Flexibility with who presents
  - Speak their language
  - Avoid technical jargon

CYNERGISTEK
Tucker Ellis LLP



Questions?

March 28, 2017

28