Financial Institutions Roundtable

A complimentary webinar series for financial institutions.

Aligning Cybersecurity and Governance:

What Directors Need to Know Now

April 13, 2016

Presented by: Terry Ammons, Partner, Porter Keadle Moore

Porter Keadle Moore

CPAs | Advisors | www.pkm.com


Threat
Bank Regulators
Cyber Resilience Measures
Information Security Forum Breach
Back Door Deception Encryption Fraud
Authentication Intrusion Version M
Challenges Linux Data Netw
Tools Protection Techn
Examinati
Vulnerab
Root9B
Resellers Controls
missions AllenVault
Security Dell SecureWorks
AVG Technolog
Forcepoin
Compliance
Pa to Networks
Trend Micro RSA
CodeDx Sophos
Cimtrak Splunk
Cisco
Cybersecurity
Overload

Integrating Cybersecurity and Governance: What a Director Needs to Know

- Objectives of Presentation
  - Board Member Responsibility
  - Top Risks to Board Members
  - Regulatory Scrutiny
  - Board Member Considerations
  - Cybersecurity Assessment Overview
  - Practical Considerations

POLLING QUESTION #1

Have you completed a risk assessment using the FFIEC's Cybersecurity Assessment Tool?

- Yes
- In progress
- No
- Unsure

Integrating Cybersecurity and Governance: What a Director Needs to Know

Integrating Cybersecurity and Governance: What a Director Needs to Know

- Top 10 Risks
  10. Existing operations not performing
  9. Customer loyalty
  8. Unexpected crisis
  7. Privacy/IS
  6. Resistance to change
  5. Culture issues
  4. Retaining top talent
  3. Cyber threats
  2. Economic conditions
  1. Regulatory scrutiny

Source | www.protiviti.com/en-US/Pages/Top-risks-survey.aspx

POLLING QUESTION #2

How involved is your Board of Directors in the cyber risk management process?

- Very involved
- Somewhat involved
- Not involved
- Unsure

Integrating Cybersecurity and Governance: What a Director Needs to Know

- Regulatory Scrutiny
  - Cyber security assessment
  - More banks downgraded
  - More regulatory orders

Integrating Cybersecurity and Governance: What a Director Needs to Know

- Risk Management Maturity
  - Operation Model
  - Who Manages the Risk
  - Risk Committee

Integrating Cybersecurity and Governance: What a Director Needs to Know

- Board Considerations for Overseeing Risk Management*
  - Know your banks top risks
  - Is Risk Management formalized
  - Does the bank have a formalized Risk Appetite Statement
  - Pre-decision Risk Evaluation

Integrating Cybersecurity and Governance: What a Director Needs to Know

- Board Considerations for Overseeing Risk Management*, continued
  - Relevant Data
  - Concept of Risk versus Rewards
  - Capturing all Risk Management Activities
  - Proper Risk Culture

* - http://www.bankdirector.com/issues/risk/how-a-board-can-credibly-challenge-management-on-risk

POLLING QUESTION #3

Does your Board have a formalized risk appetite statement?

- Yes
- No
- Unsure

Integrating Cybersecurity and Governance: What a Director Needs to Know

June 2015

https://www.ffiec.gov/cyberassessmenttool.htm

- Purpose
  - to measure cybersecurity preparedness over time
- Responsibility
  - CEO and Board Members

Integrating Cybersecurity and Governance: What a Director Needs to Know

- Cybersecurity Assessment Overview
  - Inherent Risk Profile – Least to Most
    - Technologies and connection types
    - Delivery channels
    - Online/Mobile Product and Technology Services
    - Organizational characteristics
    - External threat

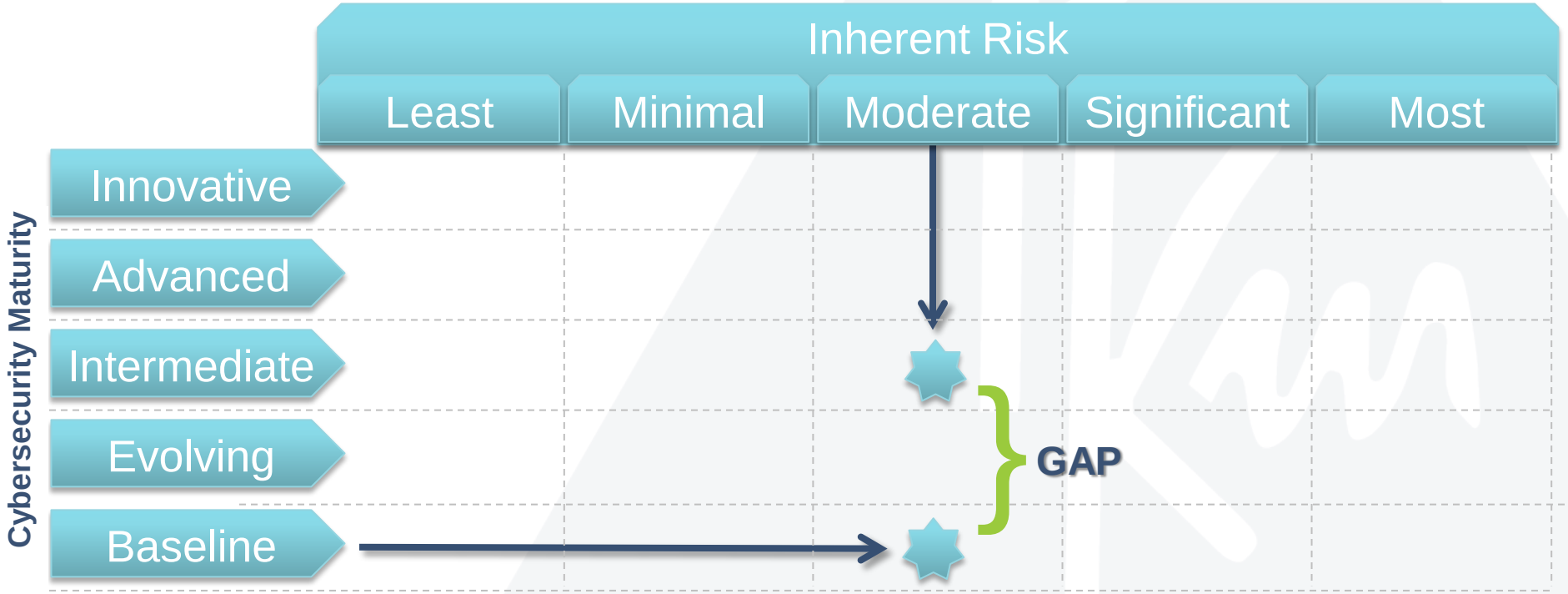
Integrating Cybersecurity and Governance: What a Director Needs to Know

- Cybersecurity Maturity
  - Baseline to Innovative
    - Cyber risk management
    - Threat intelligence and collaboration
    - Cybersecurity controls
    - External dependency management
    - Cyber incident management and resilience

Maturity is based on behaviors, practices and processes.

Integrating Cybersecurity and Governance: What a Director Needs to Know

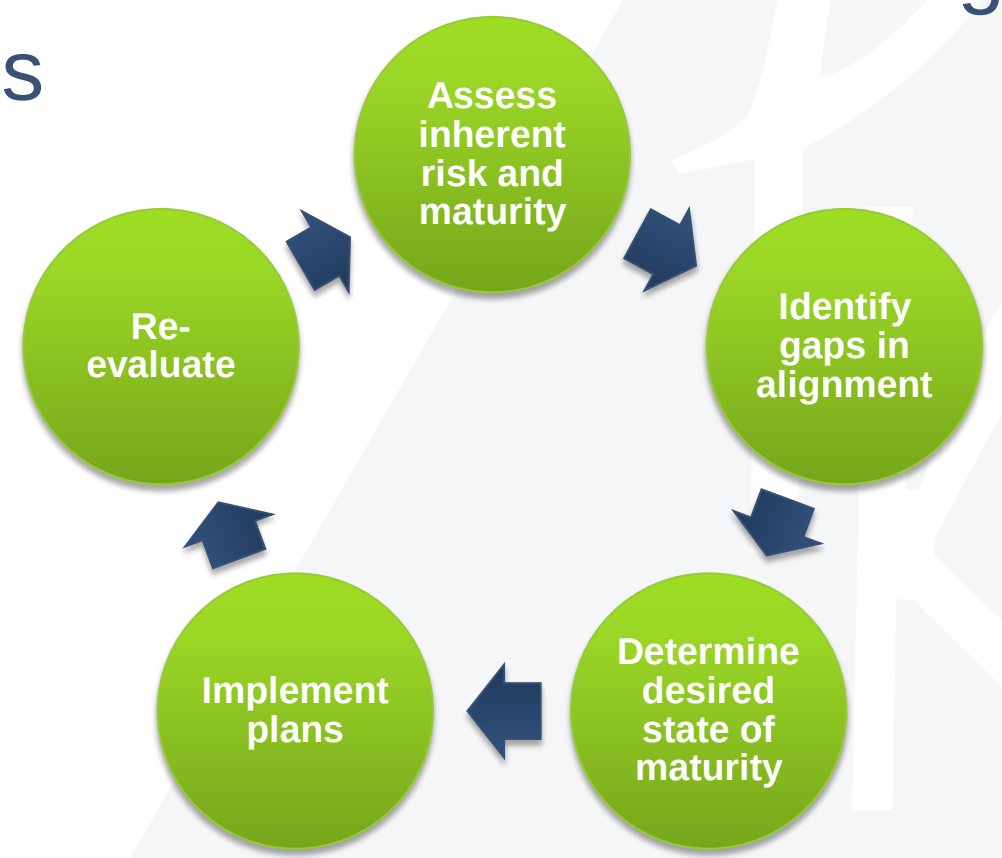
Cyber Risk Management



Gap analysis example

Integrating Cybersecurity and Governance: What a Director Needs to Know

- Cyber risk assessment as an ongoing process



POLLING QUESTION #4

Overall, do you feel the appropriate level of information is being communicated from Management to your Board?

- Yes, we do a good job
- Somewhat, could use work
- Not at all

Integrating Cybersecurity and Governance: What a Director Needs to Know

- Practical Considerations
  - Endpoints are most vulnerable
- Other items:
  - Email filtering
  - Web surfing restrictions
  - Restrict local admin rights
  - White listing – only known software/devices allowed
  - Intrusion prevention/Intrusion detection
  - User awareness training

Integrating Cybersecurity and Governance: What a Director Needs to Know

- Management/Board must do list:
  - Make sure endpoints are addressed
  - Identifying new threats/enhancing controls
  - Evaluate cyber insurance
  - Good communication to/from management/board of directors
  - Directorate is emphasizing security
  - Security controls are assessed by a third party periodically

Integrating Cybersecurity and Governance: What a Director Needs to Know

Questions?

Terry Ammons, CPA, CISA

tammons@pkm.com

Office: 404.420.5679 | Cell: 404.502.0592