# Board Oversight for Cyber Risk

Brett Tucker

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

# Notices



This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.



DM22-0627

# Agenda

- Cyber Risk Management Overview
- Why Cyber Risks Matter
- Governance Leads to Defense in Depth
- Program, Process, and Culture
- Common Questions
- Take Aways

# Oversight of Cyber Risks Matters

***Business Case For Managing Risk***

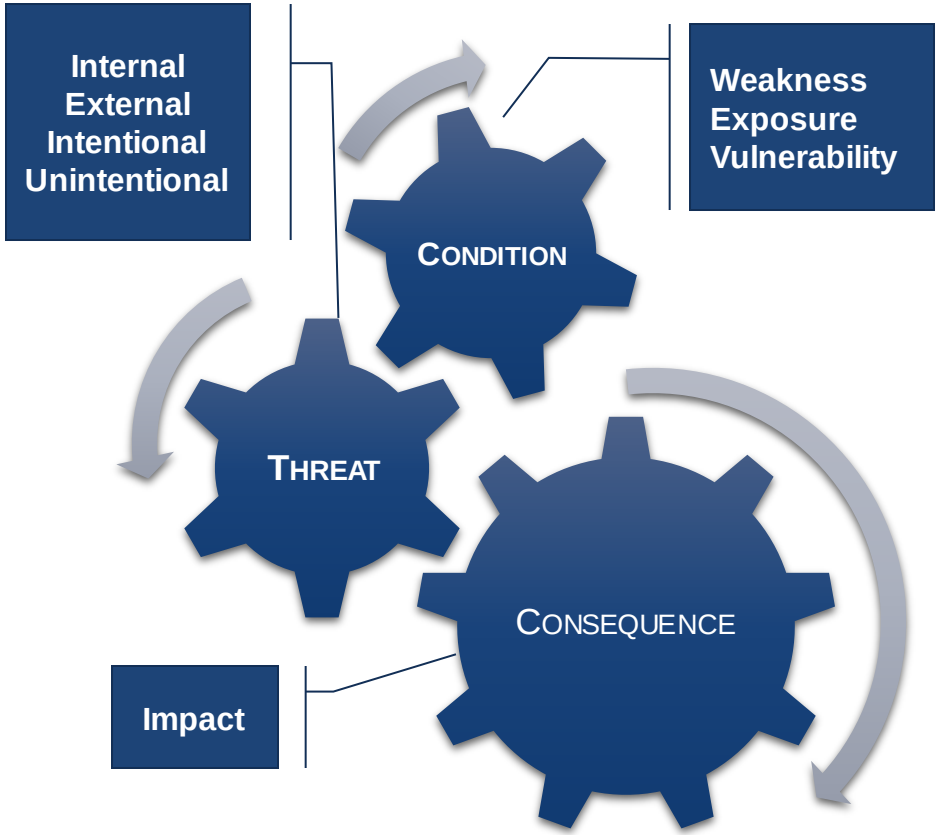
- Increases the confidence of employees and customers to improve your reputation
- Avoid compliance fines and legal penalties
- Improve customer retention
- Protect the safety of customers and employees
- Improve productivity and profitability
- Ensure operational resilience

# Key Takeaways – What is a Board Member To Do?

- Securing corporate networks, systems, and data requires persistent diligence
  - Must defend against internal and external threats.
- Adversaries constantly advance their tactics and techniques.
  - Organizations must adapt to stay ahead of emerging threat vectors.
- Boards need to prioritize control strategies based on risk-based decision making to mitigate threats.
- Board must emphasize the linkage between business objectives and risk appetite so that leadership can make risk-based decisions in a consistent manner.

# Decomposing Cyber Risk

*More Than Just an Index*



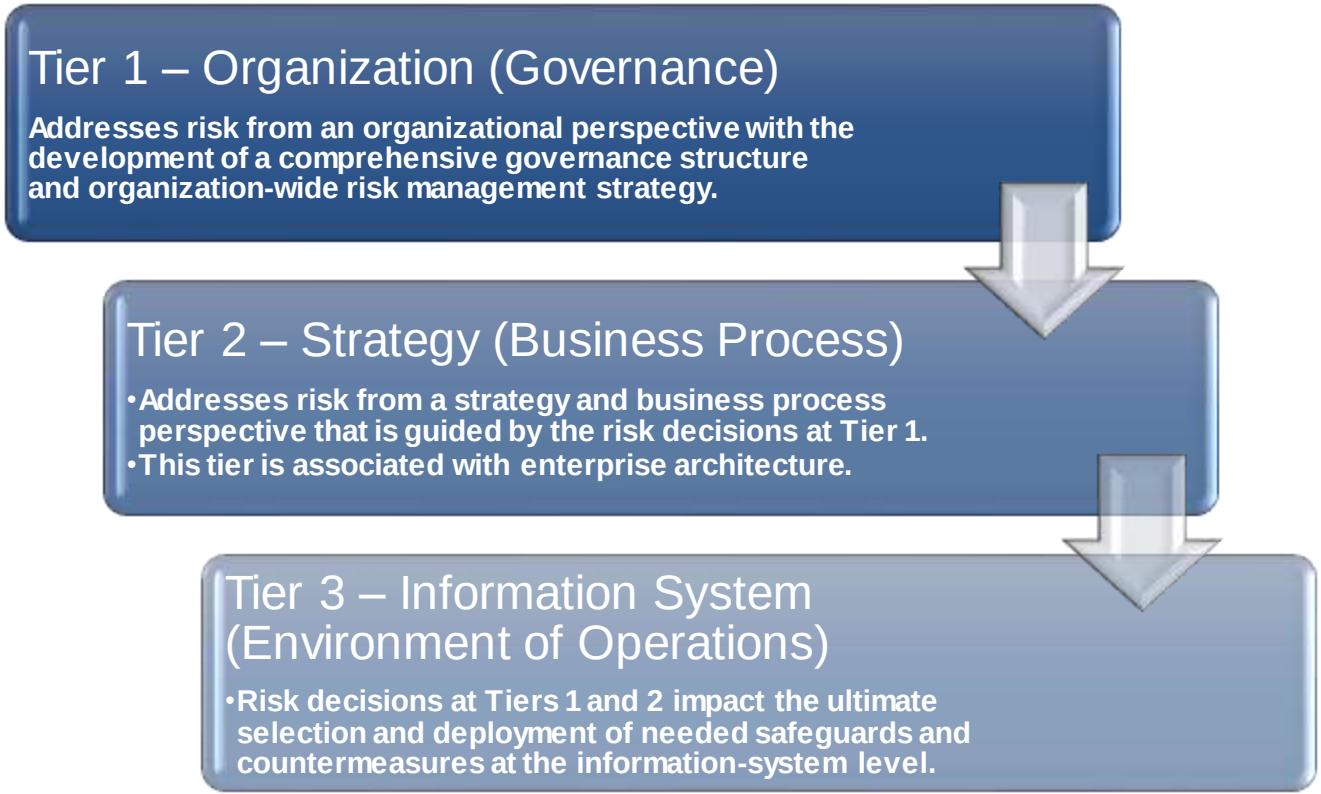

- Risk outcomes can be **positive or negative** (opportunity or threat)
- Uncertainty stems from lack of information, experience, or controllability
- Risk requires the combination of a threat and vulnerability

# **Risk Management:** A Process for Controlling Uncertainty

- **Cultural and organizational principles set the foundation** for a continuous process
  - Open communication and collaboration toward a common set of goals
- An **understanding** of
  - the organization's risk exposure
  - potential consequences of compromise
- A cyber risk response strategy must be sufficient to achieve an acceptable level of residual risk
- Organizational acceptance based on an understanding of potential consequences of residual risk – **a documented Risk Appetite is essential**
- Integration into "business as usual" – **establish a risk culture**

GOAL: ensure that business strategy and cyber strategy are aligned

# Risk Governance Leads to Defense in Depth



# Board's Role in Cybersecurity: Five Key Principles

1. Approach cybersecurity as an enterprise-wide risk management issue, not just an IT issue.

2. Understand the legal implications of cyber risks as they relate to the company's specific circumstances.

3. Have adequate access to cybersecurity expertise, hold regular discussions about cyber-risk management, and devote adequate time to the topic at board meetings.

4. Set the expectation that management will establish an enterprise-wide cyber-risk management framework with adequate staffing and budget.

5. Board-management discussions of cyber risks should include identifying which risks to avoid, accept, mitigate, or transfer through insurance, and identifying specific plans associated with each approach.

Source: NACD Director's Handbook on Cyber-Risk Oversight: www.nacdonline.org/cyber

# Creating a Cybersecurity Culture

- Tone and cadence begin at the top.

- Risk-based **decision making** comes from having a risk culture.
  - There may never be perfect protection.
  - Defined risk appetite aligns risk decisions.
  - Defensible mean that a decision was made, given the best information, and accepting risk in accordance with appetite.

- Create a set of controls to address anticipated risks for their situation and conditions.

- Controls should balance the need to protect against the need to achieve the mission.

# Cyber Risk Management Activities – What to Expect

**Organization must identify and assess risk**

- Management must hire and direct analysts to identify and craft tangible risks that are explicitly documented—qualitatively and quantitatively.

**Organization must plan a risk response**

- Determine a strategy for responding to each risk.
- Project management enables measurement of progress.

**Organization must then implement the risk response**

- Implement the plan as defined and track to completion.

# Resilience as a Business Imperative

- Cyber risk management should focus on reducing exposure and raising operational resilience.
  - Not a just technical problem.

- A structured program must support resilience—retaining operational capability despite turmoil.
  - Balance of controls that reduce risk as much as support incident response.
  - Focus on personnel behaviors and training.

- Demand full C-Suite engagement.
  - Cyber is the “silver thread” that passes through all functions.

- Performance should be gaged by the speed of response.
  - Failure to deliver on organizational objectives in a timely manner is direct loss of money.

# Common Cybersecurity Questions from the Board

- Are we keeping pace with the risk environment? How do we know?

- Where should we make our next cybersecurity investment?
  - Are we making risk-informed investments?
  - How do we demonstrate and justify the value?
  - Are we efficient (i.e., not reinventing the wheel)?

- Are we maturing in our capabilities?
  - Are processes and practices effective?

- How do we compare with our peers in the marketplace?

# Key Takeaways in Summary

Prioritize

- Set priorities and remember that if everything is the priority, then nothing is priority.
- Not all threats, vulnerabilities, and assets are equal—analyze and measure where possible.
- Select the most cost-effective controls to conserve resources.
- Strategies vary based upon confidentiality, integrity, and availability.

Specialize

- Know your enemy and your environment.
- Target high frequency vectors like spear phishing and ransomware.
- Tailor your security program to your organizational strategy.
- Develop an implementation roadmap.

# Contact Information

Brett Tucker, PMP, CSSBB, CISSP, CAP

Technical Manager, Cyber Risk Management

Telephone: 412.268.6682

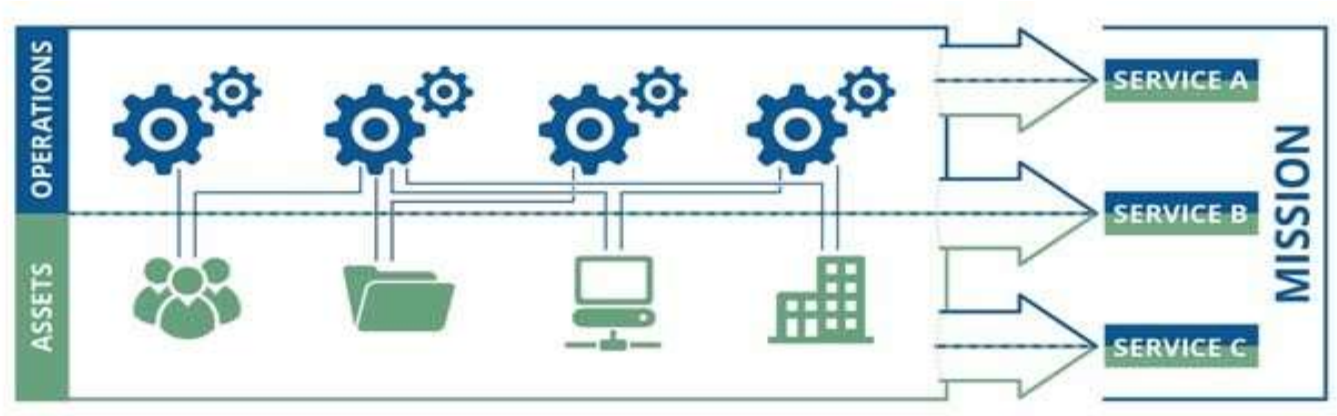
Email: batucker@cert.org

# Establishing Risk Management Context

**Define:**

- Organization, **process**, project or activity (to be assessed)
  - Establish goals/objectives
  - Determine duration of the project, activity, or function
- Full scope of risk management **activities** to be carried out
  - Specify inclusions and exclusions
- **Roles and responsibilities** of the various participants in the risk management process
- Dependencies among the project or activity and other projects or parts of the organization

# Link Cybersecurity to Business Objectives




**People**: those who operate and monitor the service
**Information**: data associated with the service
**Technology**: tools and equipment that automate and support the service
**Facilities**: where the service is performed
**External Dependencies**: value gained from relationships/supply chain

**! Assets derive their value from their importance in meeting the service mission.**

# Cyber Risk Management

NIST SP 800-30

- Defines **risk** as "a function of the ***likelihood*** of a given ***threat-source*** exercising a particular potential ***vulnerability, and*** the resulting ***impact*** of that adverse event on the organization"
  - threat-source – natural, human, or environmental
  - threat – potential for threat-source to exploit vulnerability
  - vulnerability – flaw that can present a security breach
  - likelihood – probability of threat combining with vulnerability
  - countermeasure – control to reduce risk

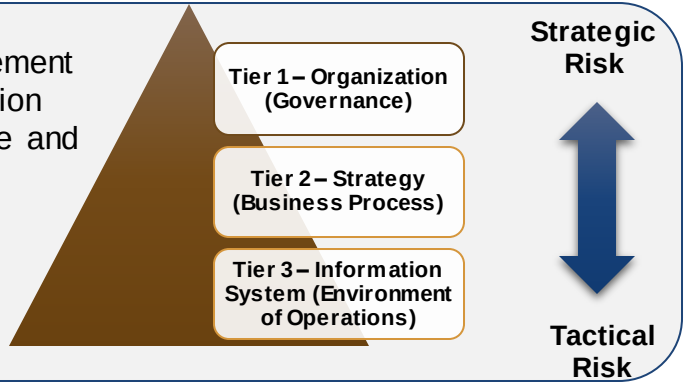
At a high level, cyber risk management is accomplished by **balancing exposure** to risks **against cost** of mitigation and implementing appropriate countermeasures and controls.

# Tiers of Cyber Risk Management

Cyber risk management can be viewed as a **holistic activity** that is fully integrated into every aspect of the organization:

- organization level
- strategy and business process level
- information system level

- Multi-tier organization-wide risk management
- Implemented by the risk executive function
- Tightly coupled to enterprise architecture and information security architecture
- System development lifecycle focus
- Disciplined and structured process
- Flexible and agile implementation




Ref: NIST SP 800-39

# Models and Frameworks

- NIST Cybersecurity Framework for Critical Infrastructure
- ISACA COBIT 5.0 – Now updated as COBIT 2019
- NIST 800 Series Special Publications
- ISO 27000 family of publications
- ISO 31000 family of publications
- Maturity Models (e.g., CERT-RMM)

# Questions a Board Should Ask the CISO - 1

- What are our critical assets?
- Have we effectively allocated resources based on our risk appetite and strategic assets?
- Do we have an enterprise-wide risk management framework in place with adequate staffing and budget?
- What are our biggest risks and vulnerabilities?
- Who has access to our assets? Do third parties have access?
- What technical capabilities do we have in place to identify malicious events in real time?

# Questions a Board Should Ask the CISO - 2

- What is our response plan in the event of a breach or attack?
  - How often do we test the response plan?
- What relationships do we have with law enforcement and other third-party organizations to respond effectively to a breach?
- What kind of cyber threat information sharing does the business participate in?
  - With whom does the business exchange this information?
- What relationships need to be developed (i.e., with government agencies or other constituencies)?
- How do we compare to our peers (e.g., competitors, sector, organizations of similar size, geographic region)?