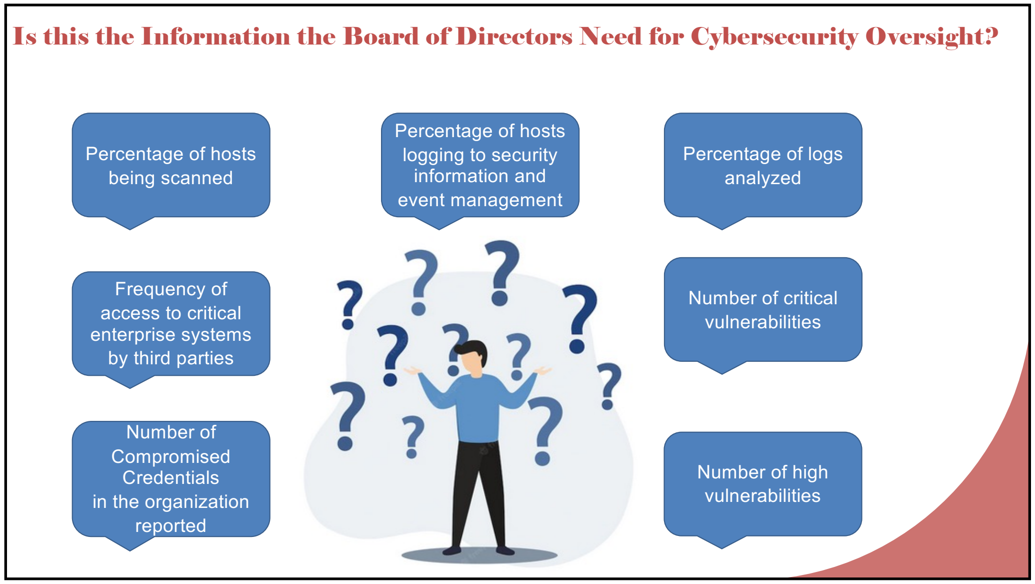
Cybersecurity at MIT Sloan

Balanced Scorecard On Cybersecurity Resilience for Board Members

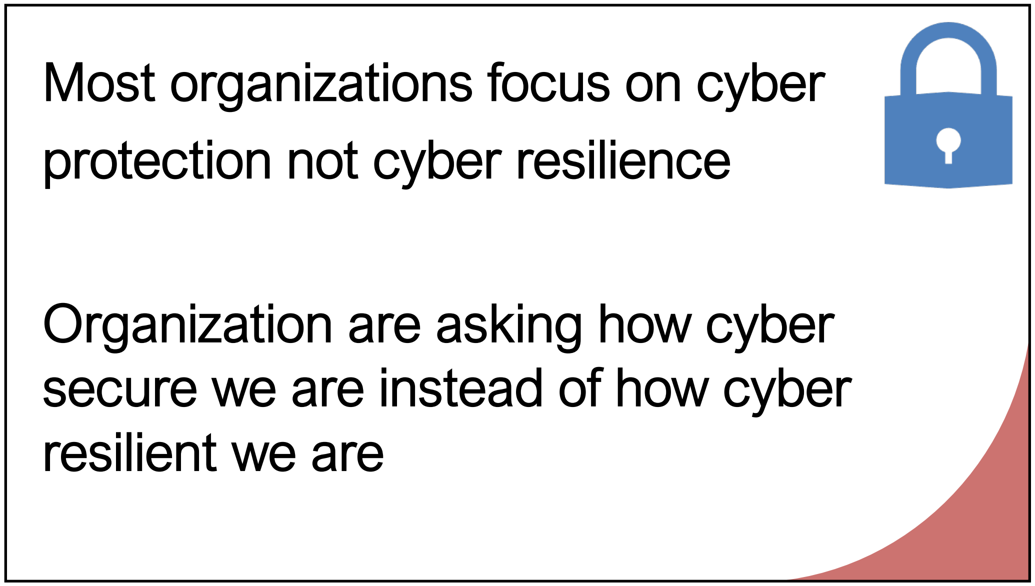
1



Is this the Information the Board of Directors Need for Cybersecurity Oversight?

- Percentage of hosts being scanned
- Percentage of hosts logging to security information and event management
- Percentage of logs analyzed
- Frequency of access to critical enterprise systems by third parties
- Number of critical vulnerabilities
- Number of Compromised Credentials in the organization reported
- Number of high vulnerabilities

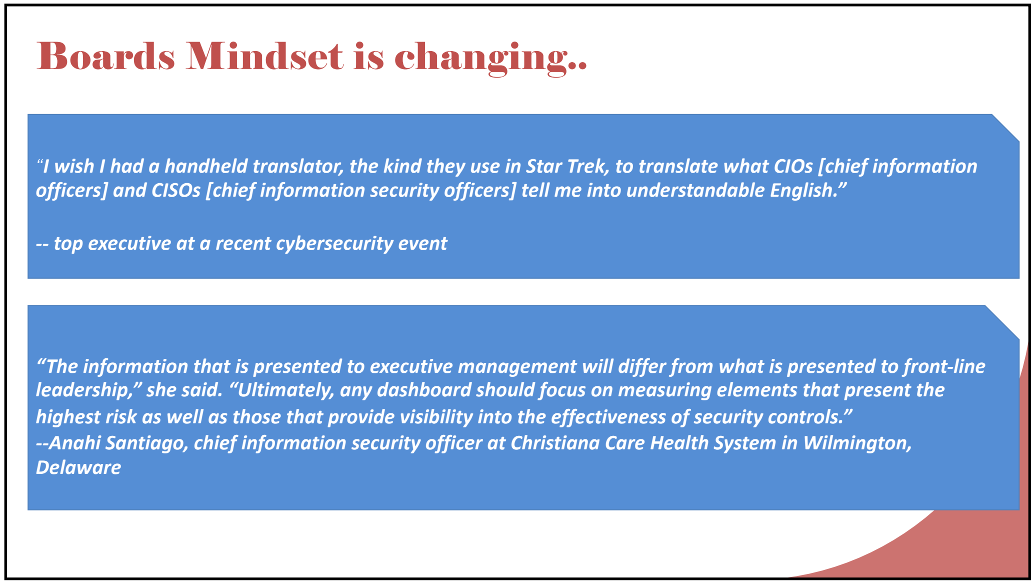
2



Most organizations focus on cyber protection not cyber resilience

Organization are asking how cyber secure we are instead of how cyber resilient we are

3



Boards Mindset is changing..

“I wish I had a handheld translator, the kind they use in Star Trek, to translate what CIOs [chief information officers] and CISOs [chief information security officers] tell me into understandable English.”

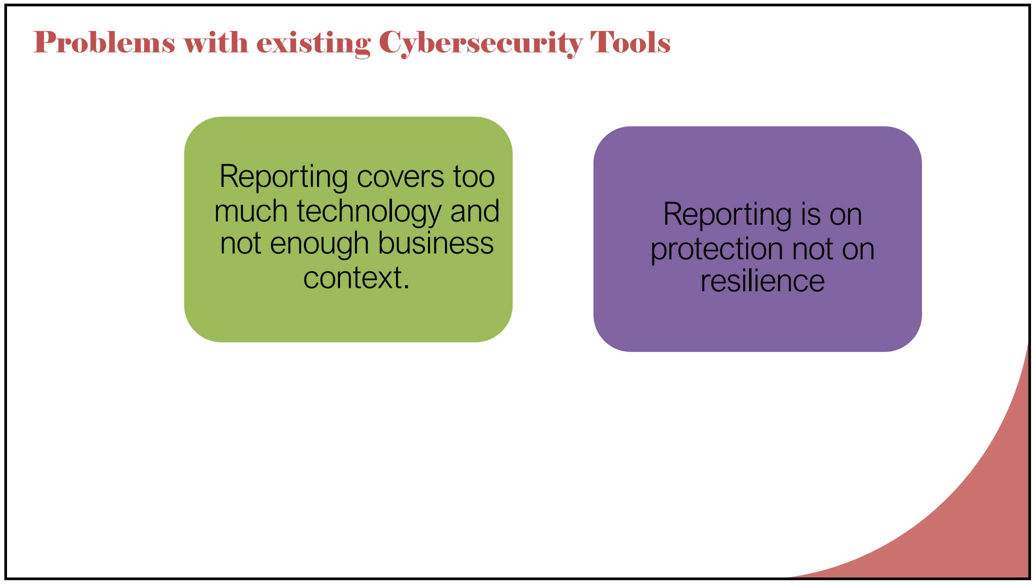
-- top executive at a recent cybersecurity event

“The information that is presented to executive management will differ from what is presented to front-line leadership,” she said. “Ultimately, any dashboard should focus on measuring elements that present the highest risk as well as those that provide visibility into the effectiveness of security controls.”
--Anahi Santiago, chief information security officer at Christiana Care Health System in Wilmington, Delaware

4

Boards have oversight and fiduciary responsibility to help organizations make better business decisions and manage risks

5



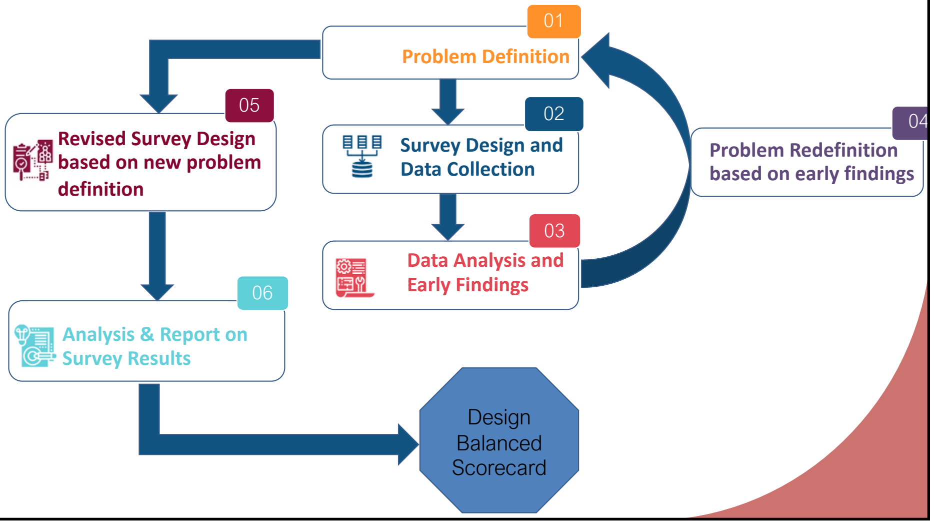
Problems with existing Cybersecurity Tools

Reporting covers too much technology and not enough business context.

Reporting is on protection not on resilience

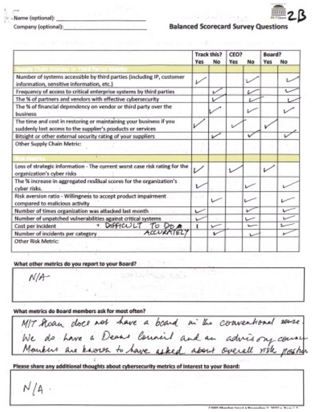
6

Research Process


01
Problem Definition
02
Survey Design and Data Collection
03
Data Analysis and Early Findings
04
Problem Redefinition based on early findings
05
Revised Survey Design based on new problem definition
06
Analysis & Report on Survey Results
Design Balanced Scorecard

7

Data Collection - Survey Results



Name (optional): __________________

Company (optional): __________________

2B

Balanced Scorecard Survey Questions

	Track this?		CEO?		Board?	
	Yes	No	Yes	No	Yes	No
Supply Chain (Vendor or Third Party) Metrics						
Number of systems accessible by third parties (including IP, customer information, sensitive information, etc.)	✓			✓		✓
Frequency of access to critical enterprise systems by third parties		✓		✓		✓
The % of partners and vendors with effective cybersecurity		✓		✓		✓
The % of financial dependency on vendor or third party over the business		✓		✓		✓
The time and cost in restoring or maintaining your business if you suddenly lost access to the supplier's products or services	✓		✓		✓	
Bitsight or other external security rating of your suppliers		✓		✓		✓
Other Supply Chain Metric:						
Risk Metrics						
Loss of strategic information - The current worst case risk rating for the organization's cyber risks	✓		✓		✓	
The % increase in aggregated residual scores for the organization's cyber risks.	✓			✓		✓
Risk aversion ratio - Willingness to accept product impairment compared to malicious activity		✓		✓		✓
Number of times organization was attacked last month	✓			✓		✓
Number of unpatched vulnerabilities against critical systems	✓			✓		✓
Cost per incident • DIFFICULT TO DO A ACCURATELY	I	✓		✓		✓
Number of incidents per category		✓		✓		✓
Other Risk Metric:						

What other metrics do you report to your Board?

N/A

What metrics do Board members ask for most often?

MIT Sloan does not have a board in the conventional sense. We do have a Deans Council and an advisory council. Members are known to have asked about overall risk position

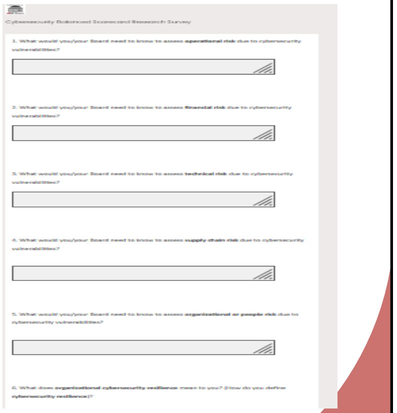
Please share any additional thoughts about cybersecurity metrics of interest to your Board:

N/A

CAMS Member Input • November 2, 2022 • Page 1 | 2

Survey 1

Survey evolved during course of the research



Cybersecurity Balanced Scorecard Research Survey

1. What would you/your Board need to know to assess **operational risk** due to cybersecurity vulnerabilities?

2. What would you/your Board need to know to assess **financial risk** due to cybersecurity vulnerabilities?

3. What would you/your Board need to know to assess **technical risk** due to cybersecurity vulnerabilities?

4. What would you/your Board need to know to assess **supply chain risk** due to cybersecurity vulnerabilities?

5. What would you/your Board need to know to assess **organizational or people risk** due to cybersecurity vulnerabilities?

6. What does **organizational cybersecurity resilience** mean to you? (How do you define **cybersecurity resilience**)?

Survey 2

https://bit.ly/CAMSScorecard

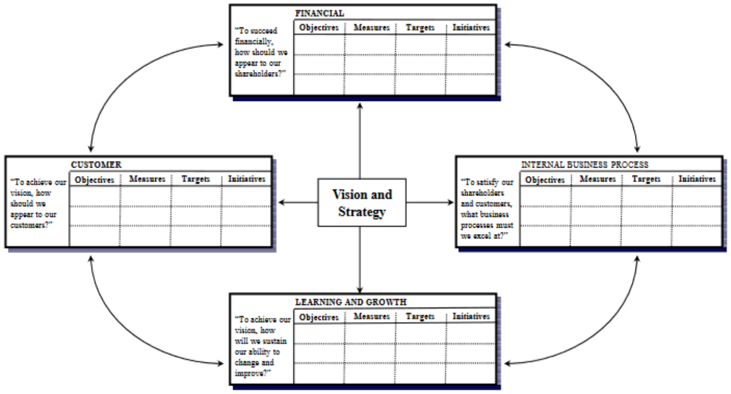
8

Sample Questions asked in revised survey regarding Organizational Resilience

1. What would you/your Board need to know to **assess organizational risk** due to cybersecurity vulnerabilities?
2. What would you/your Board need to know to **assess overall organizational resilience** to cybersecurity vulnerabilities?
3. What do you/your **Board discuss** today when the Board reviews Cybersecurity for the organization?
4. What does the Board need to know to **assess how ready the organization is to weather a cybersecurity incident**?
5. What questions does the Board **ask of the Cybersecurity leaders** in Board meetings today?

9

Conceptual Foundation of a Balanced Scorecard



FINANCIAL

"To succeed financially, how should we appear to our shareholders?"

Objectives	Measures	Targets	Initiatives

CUSTOMER

"To achieve our vision, how should we appear to our customers?"

Objectives	Measures	Targets	Initiatives

Vision and Strategy

INTERNAL BUSINESS PROCESS

"To satisfy our shareholders and customers, what business processes must we excel at?"

Objectives	Measures	Targets	Initiatives

LEARNING AND GROWTH

"To achieve our vision, how will we sustain our ability to change and improve?"

Objectives	Measures	Targets	Initiatives

**Source: 1992 Harvard Business Review article (Kaplan & Norton, 1992)

10

Developing a Balanced Scorecard: Our Vision

It's resilience we need to focus on:
How resilient are we to a cyber incident/breach/attack.

There are several dimensions that contribute to resiliency.

The most important questions the balanced scorecard helps to answer will be:

1. How resilient to a cyber incident/breach/attack are we?
2. What is our overall cybersecurity spend? What is our biggest expense?
3. What is our biggest organizational risk (likely phishing)? How are we managing it?
4. What is our biggest technological risk? How are we managing it?
5. What is our biggest supply chain risk? How are we managing it?

11

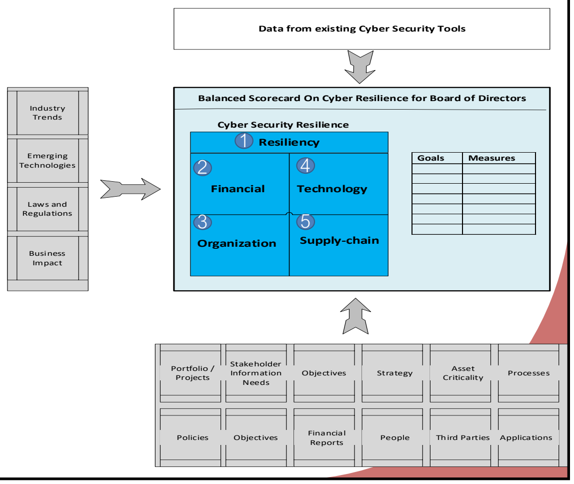
Developing a Balanced Scorecard: Our Vision

It's resilience we need to focus on:
How resilient are we to a cyber incident/breach/attack.

There are several dimensions that contribute to resiliency.

The most important questions the balanced scorecard helps to answer will be:

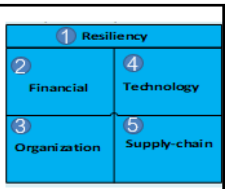
1. How resilient to a cyber incident/breach/attack are we?
2. What is our overall cybersecurity spend? What is our biggest expense?
3. What is our biggest organizational risk (likely phishing)? How are we managing it?
4. What is our biggest technological risk? How are we managing it?
5. What is our biggest supply chain risk? How are we managing it?



12

Discussion Questions for Today

1. What do you think is the difference between cyber protection and cyber resilience?
2. How do you measure people side of cyber resilience today?
3. What does your board need to know about organization's cyber resilience?
4. Any feedback on balanced scorecard?


1 Resiliency
2 Financial
4 Technology
3 Organization
5 Supply-chain

Balanced Scorecard

14

Thank You

15