Five Key Factors Defining Your Board Engagement Strategy

Mark Grimse

VP IT, Rambus

splunk>

Disclaimer

During the course of this presentation, we may make forward looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC. The forward-looking statements made in the this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward looking statements we may make.

In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not, be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.

Personal Introduction

- Mark Grimse, Rambus
- Rambus creates cutting-edge semiconductor and IP products, spanning memory and interfaces to security, smart sensors and lighting
- ~500 Employees (~70% engineers)
- 5 Major design centers WW
- WW IT Responsible for all internal systems, desktops/laptops, BYOD, networks, storage, servers, and compute farm

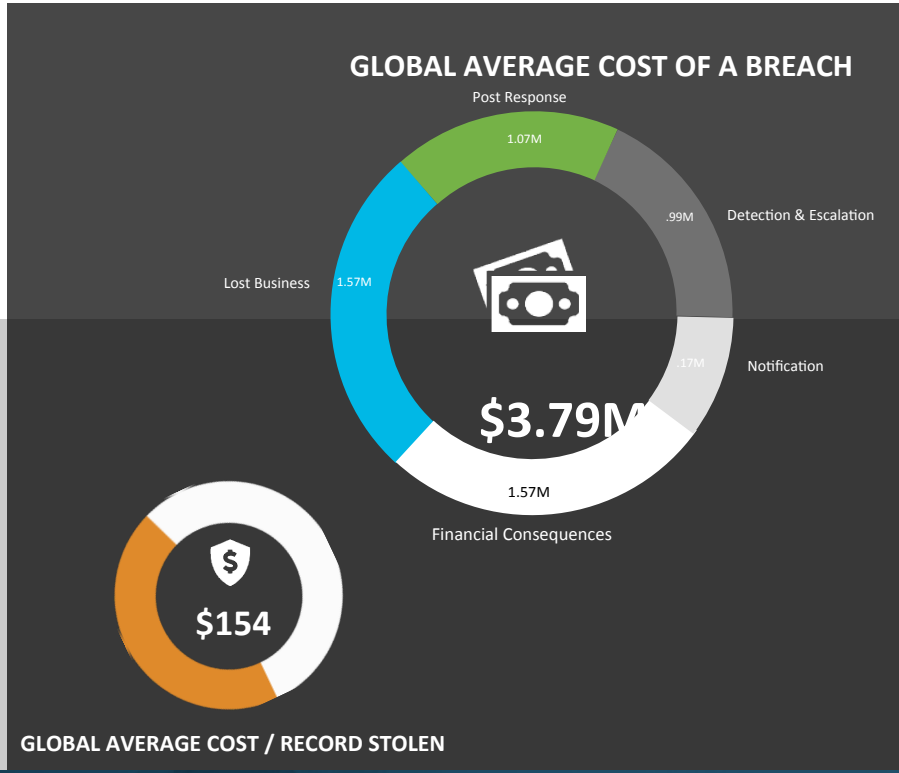
Agenda

- The Problem
- Our Approach
- Key Examples For Validation
- Forward Action
- Q&A

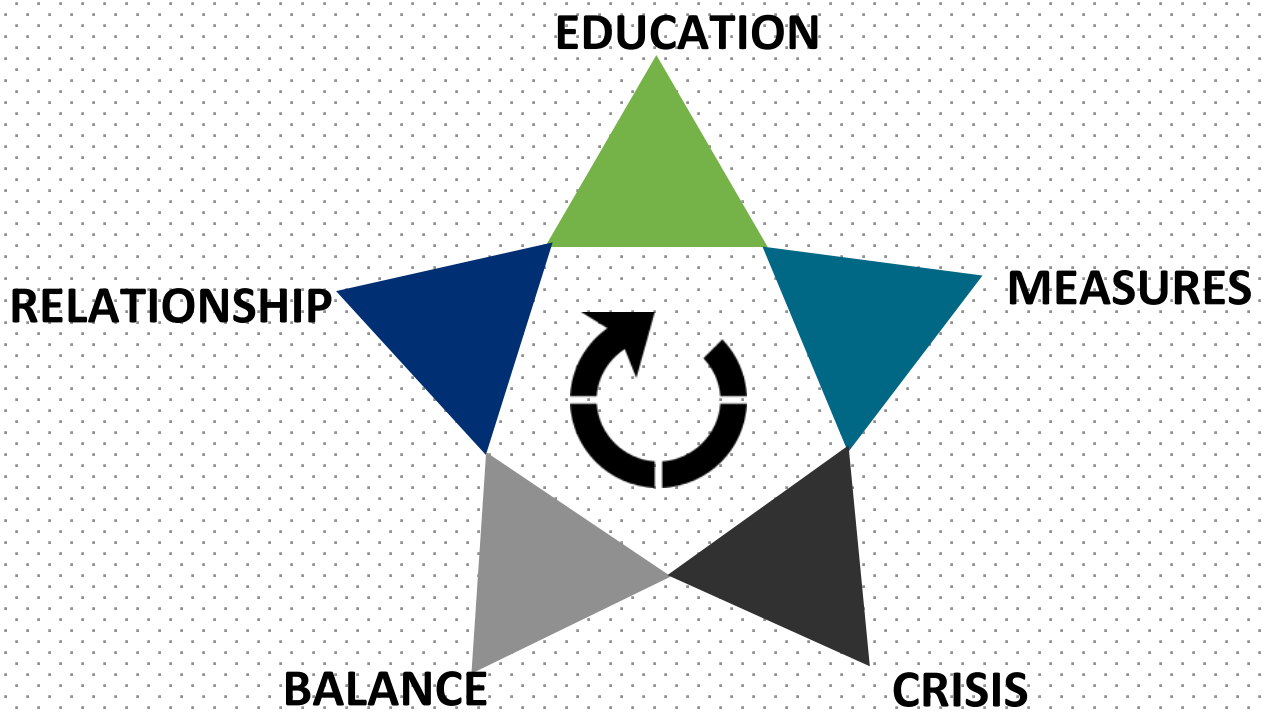
How many of your Boards are capable of understanding your companies Cyber-security posture and response capabilities?

The Problem

Today's Board of Directors are ill-equipped to provide valuable feedback to the CIO regarding cyber security risk management. The capability gap reduces a company's ability to appropriately manage and respond to modern cyber risks.



RISK – 4Ps

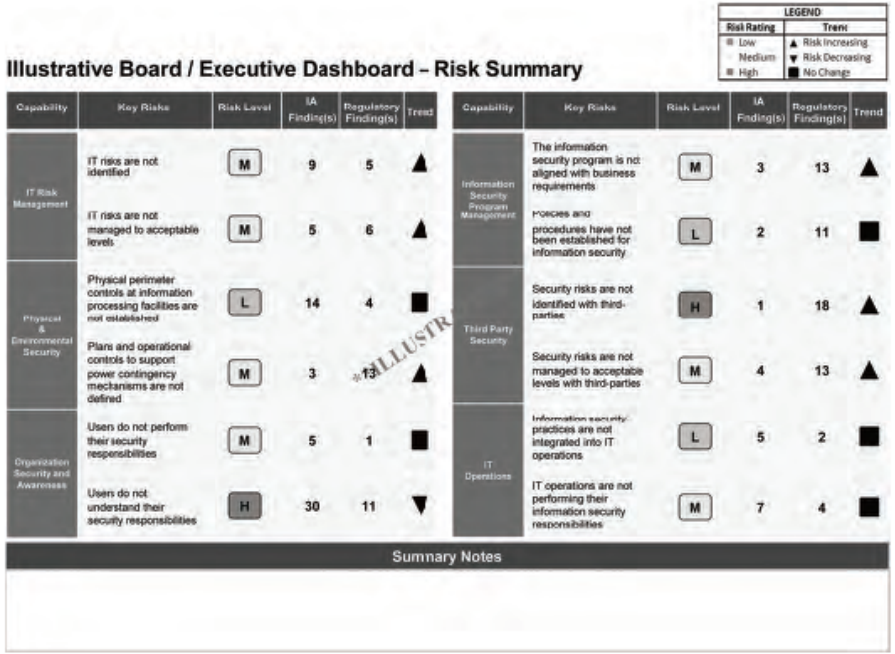

EDUCATION
RELATIONSHIP
MEASURES
BALANCE
CRISIS

Education

- Define – do they understand, have you talked to them and have reassurance they do? Board assessment?
- What to know – risk vs costs, terminology, specific threats to your company and industry
- How to teach Articles/links to them, special session, private 1-1, outside speakers

Measures

- What a BOD needs
- Less than perfect solution today + how to evolve
- Type of measures
  - Qualitative – from NACD Cyber-risk oversight handbook
- Quantitative
  - Some of the Sans top 20 measures



Illustrative Board / Executive Dashboard – Risk Summary

LEGEND

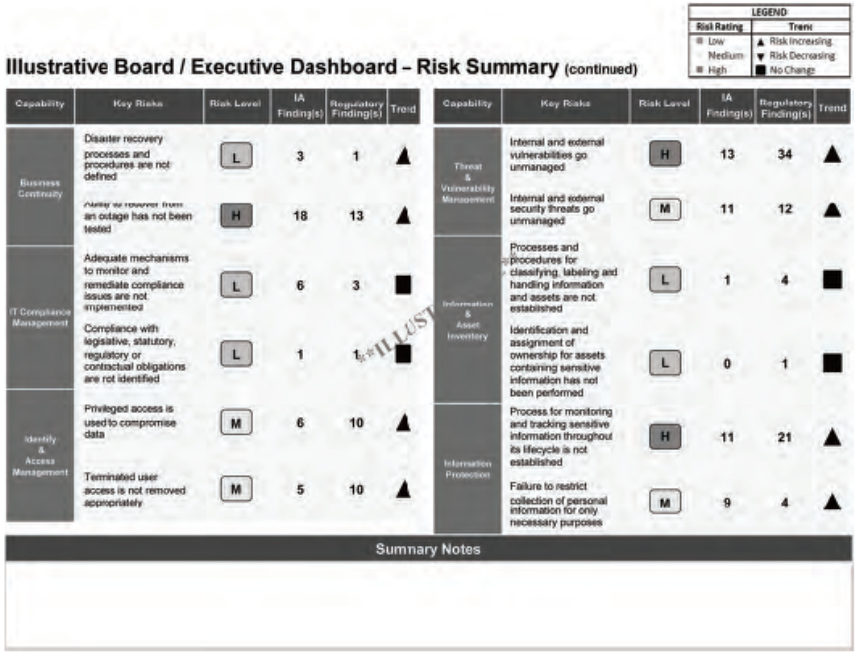
Risk Rating	Trend
Low	▲ Risk Increasing
Medium	▼ Risk Decreasing
High	■ No Change

Capability	Key Risks	Risk Level	IA Finding(s)	Regulatory Finding(s)	Trend
IT Risk Management	IT risks are not identified	M	9	5	▲
	IT risks are not managed to acceptable levels	M	5	6	▲
Physical & Environmental Security	Physical perimeter controls at information processing facilities are not established	L	14	4	■
	Plans and operational controls to support power contingency mechanisms are not defined	M	3	13	▲
Organization Security and Awareness	Users do not perform their security responsibilities	M	5	1	■
	Users do not understand their security responsibilities	H	30	11	▼

Capability	Key Risks	Risk Level	IA Finding(s)	Regulatory Finding(s)	Trend
Information Security Program Management	The information security program is not aligned with business requirements	M	3	13	▲
	Policies and procedures have not been established for information security	L	2	11	■
Third Party Security	Security risks are not identified with third-parties	H	1	18	▲
	Security risks are not managed to acceptable levels with third-parties	M	4	13	▲
IT Operations	Information security practices are not integrated into IT operations	L	5	2	■
	IT operations are not performing their information security responsibilities	M	7	4	■

Summary Notes

Measures



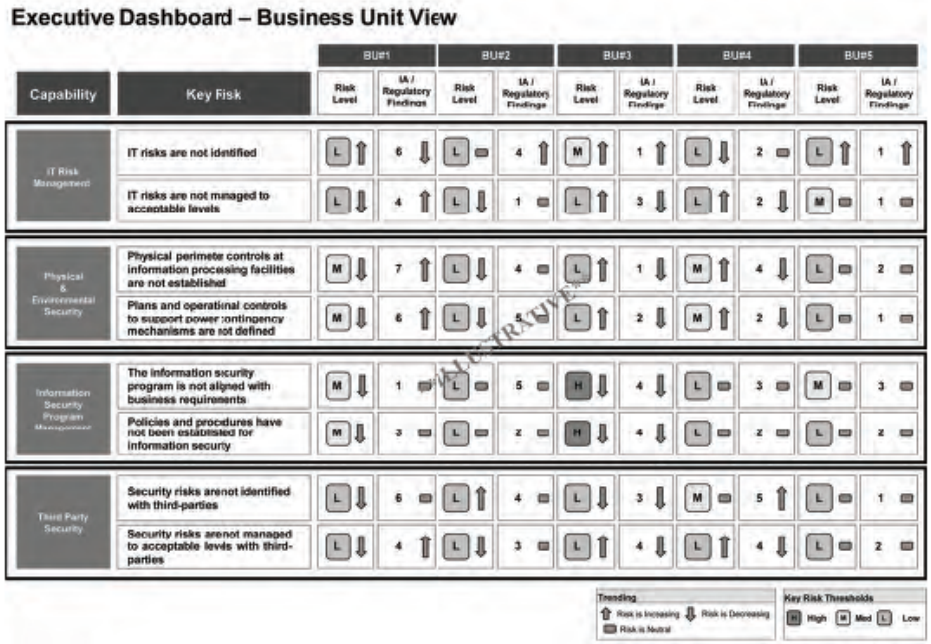
Illustrative Board / Executive Dashboard – Risk Summary (continued)

LEGEND

Risk Rating	Trend
Low	Risk Increasing
Medium	Risk Decreasing
High	No Change

Capability	Key Risks	Risk Level	IA Finding(s)	Regulatory Finding(s)	Trend
Business Continuity	Disaster recovery processes and procedures are not defined	L	3	1	▲
	Ability to recover from an outage has not been tested	H	18	13	▲
IT Compliance Management	Adequate mechanisms to monitor and remediate compliance issues are not implemented	L	6	3	■
	Compliance with legislative, statutory, regulatory or contractual obligations are not identified	L	1	1	■
Identity & Access Management	Privileged access is used to compromise data	M	6	10	▲
	Terminated user access is not removed appropriately	M	5	10	▲
Threat & Vulnerability Management	Internal and external vulnerabilities go unmanaged	H	13	34	▲
	Internal and external security threats go unmanaged	M	11	12	▲
Information & Asset Inventory	Processes and procedures for classifying, labeling and handling information and assets are not established	L	1	4	■
	Identification and assignment of ownership for assets containing sensitive information has not been performed	L	0	1	■
Information Protection	Process for monitoring and tracking sensitive information throughout its lifecycle is not established	H	11	21	▲
	Failure to restrict collection of personal information for only necessary purposes	M	9	4	▲

Sumnary Notes



Executive Dashboard – Business Unit View

Capability	Key Risk	BU#1 Risk Level	BU#1 IA / Regulatory Findings	BU#2 Risk Level	BU#2 IA / Regulatory Findings	BU#3 Risk Level	BU#3 IA / Regulatory Findings	BU#4 Risk Level	BU#4 IA / Regulatory Findings	BU#5 Risk Level	BU#5 IA / Regulatory Findings
IT Risk Management	IT risks are not identified	L ⇑	6 ⇓	L ▬	4 ⇑	M ⇑	1 ⇑	L ⇓	2 ▬	L ⇑	1 ⇑
	IT risks are not managed to acceptable levels	L ⇓	4 ⇑	L ⇓	1 ▬	L ⇑	3 ⇓	L ⇑	2 ⇓	M ▬	1 ▬
Physical & Environmental Security	Physical perimete controls at information processing facilities are not established	M ⇓	7 ⇑	L ⇓	4 ▬	L ⇑	1 ⇓	M ⇑	4 ⇓	L ▬	2 ▬
	Plans and operational controls to support power contingency mechanisms are not defined	M ⇓	6 ⇑	L ⇓	5 ▬	L ⇑	2 ⇓	M ⇑	2 ⇓	L ▬	1 ▬
Information Security Program Management	The information security program is not aligned with business requirements	M ⇓	1 ▬	L ▬	5 ▬	H ⇓	4 ⇓	L ▬	3 ▬	M ▬	3 ▬
	Policies and procedures have not been established for information security	M ⇓	3 ▬	L ▬	2 ▬	H ⇓	4 ⇓	L ▬	2 ▬	L ▬	2 ▬
Third Party Security	Security risks arenot identified with third-parties	L ⇓	6 ▬	L ⇑	4 ▬	L ⇓	3 ⇓	M ▬	5 ⇑	L ▬	1 ▬
	Security risks arenot managed to acceptable levels with third-parties	L ⇓	4 ⇑	L ⇓	3 ▬	L ⇑	4 ⇓	L ⇑	4 ⇓	L ▬	2 ▬

Trending: ⇑ Risk is Increasing ⇓ Risk is Decreasing ▬ Risk is Neutral

Key Risk Thresholds: H High M Med L Low

Crisis

BOD Role

Ownership

Advisor from BoD

Advisor to BoD

Balance

Define

Investment Risk

Ease of use and secure

Relationship

- ✓ Working relationship with Board
- ✓ Value from previous steps
- ✓ Agenda item
- ✓ Drive by relationship

Forward Action

- CIO – What Can CISO and Sys admins do to support your CIO's board efforts?
- Board Assessment
- Get on agenda…somehow, be proactive not reactive

Questions?

THANK YOU

splunk>