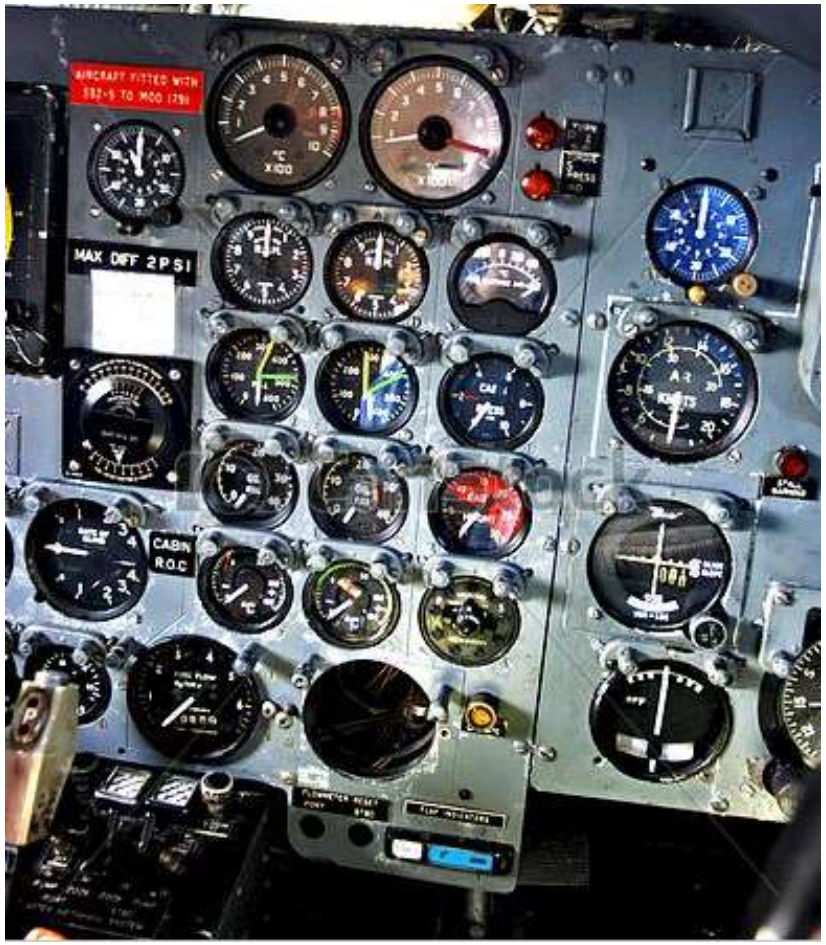
Technology Risk and Cybersecurity Metrics for Your Board

Srinath Sampath

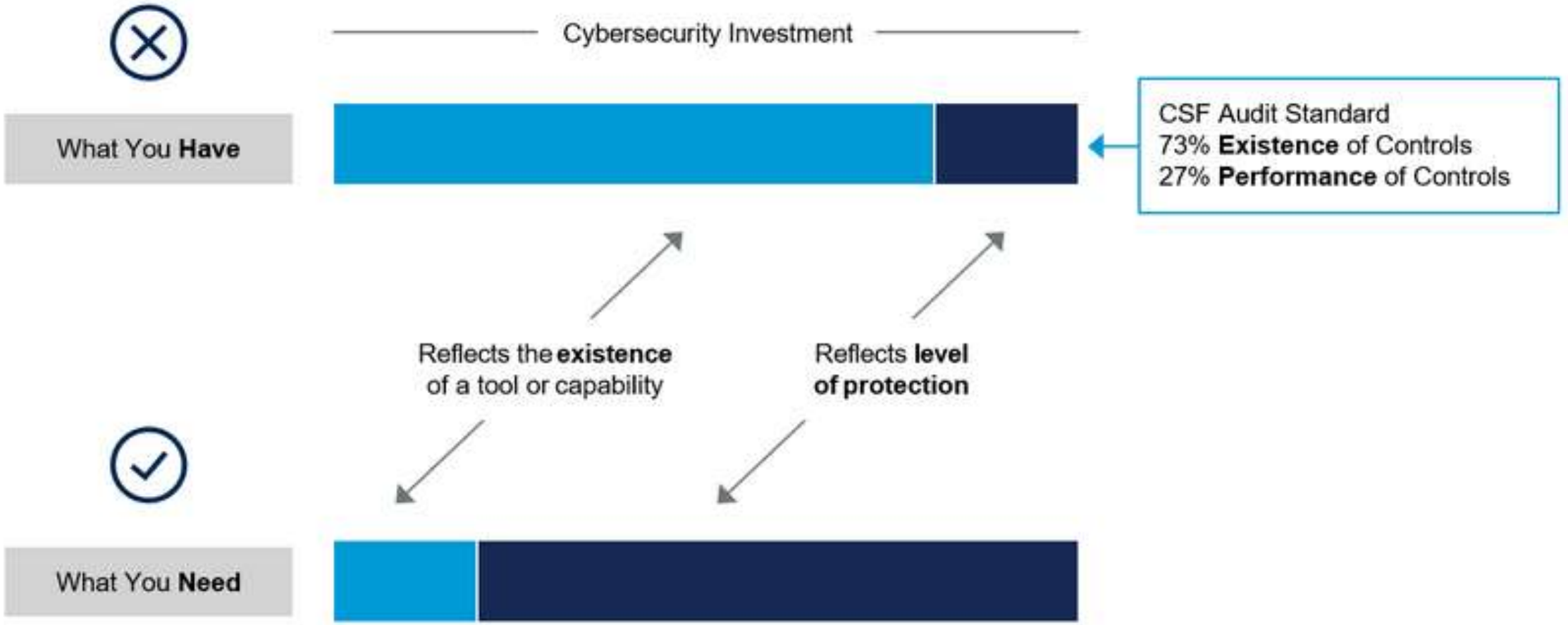
Gartner®

What Does the Passenger Need to Know?



Gartner

The Failure of Cybersecurity Investment



Typical Metrics Being Reported Today

Metric	Value Assessment and Limitations
Percentage of hosts logging to security information and event management	Good coverage metric; guides investment; not an outcome
Percentage of logs analyzed	Limited coverage metric; informs investment; not an outcome
Number of critical vulnerabilities	Trailing indicator; at worst misleads investment
Number of high vulnerabilities	Trailing indicator; at worst misleads investment
Percentage of hosts being scanned	Weak coverage metric; many levels removed from the outcome

Greater Scrutiny on Technology Risk

High-Profile Data Breaches Growing in Frequency and Scale

Heightened Scrutiny on Board's Information Risk Oversight Responsibilities

"Boards that choose to ignore, or minimize, the importance of cybersecurity responsibility do so at their own peril."

Luis A. Aguilar
US SEC Commissioner

Information Security Rises to the Top of Board Agenda

60%

Directors Believe Board is More Involved in Cybersecurity Today Than it was 12 Months Ago

Pressure on CISOs to Address Board's Information Security Concerns

65%

CISOs Present 2–4 Times or More in a Year to the Board Now

Gartner

A New Era of Risk Reporting to the Board

Frequency of Interactions	The majority of CISOs are presenting 2 to 4 times or more in a year, and often to the full board rather than a subcommittee.
Intensity of Interactions	Discussions have moved away from security metrics and annual program reporting to understanding the true nature and enterprisewide ramifications of information security risks.
Level of Audience Awareness and Sensitivity	Board members are increasingly aware and concerned about the importance of information security
Greater Individual Stake	Suddenly directors face potential removal and lawsuits based on theories of breach of fiduciary duty and corporate waste arising from costly security incidents.

What Is Appropriate Risk?

There is no such thing as "perfect protection"

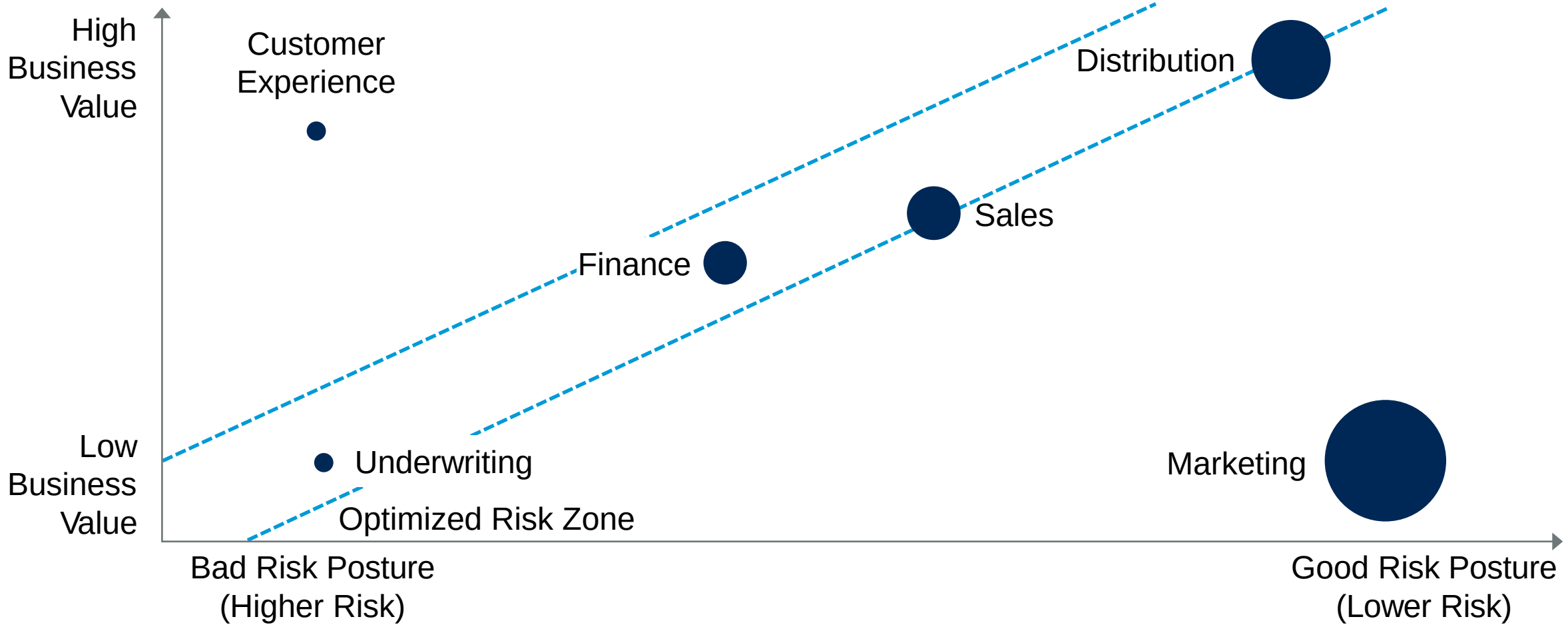
Higher Risk
Lower Investment

Lower Risk
Higher Investment

Our goal is to build a sustainable program that balances the need to protect against the needs to run our business.

Optimize Risk, Value, Cost by Business Function

X-Axis = Risk, Y-Axis = Value, Size of Bubble = Cost



The Spectrum of Measurement

Measure What Has Already Happened

Measure the Risk Exposure to Potential Events

Subjective Assessment by Subject-Matter Experts

Expected Currency Value of Loss Exposure

Operational Performance Measures

Business Outcome-Focused Measures

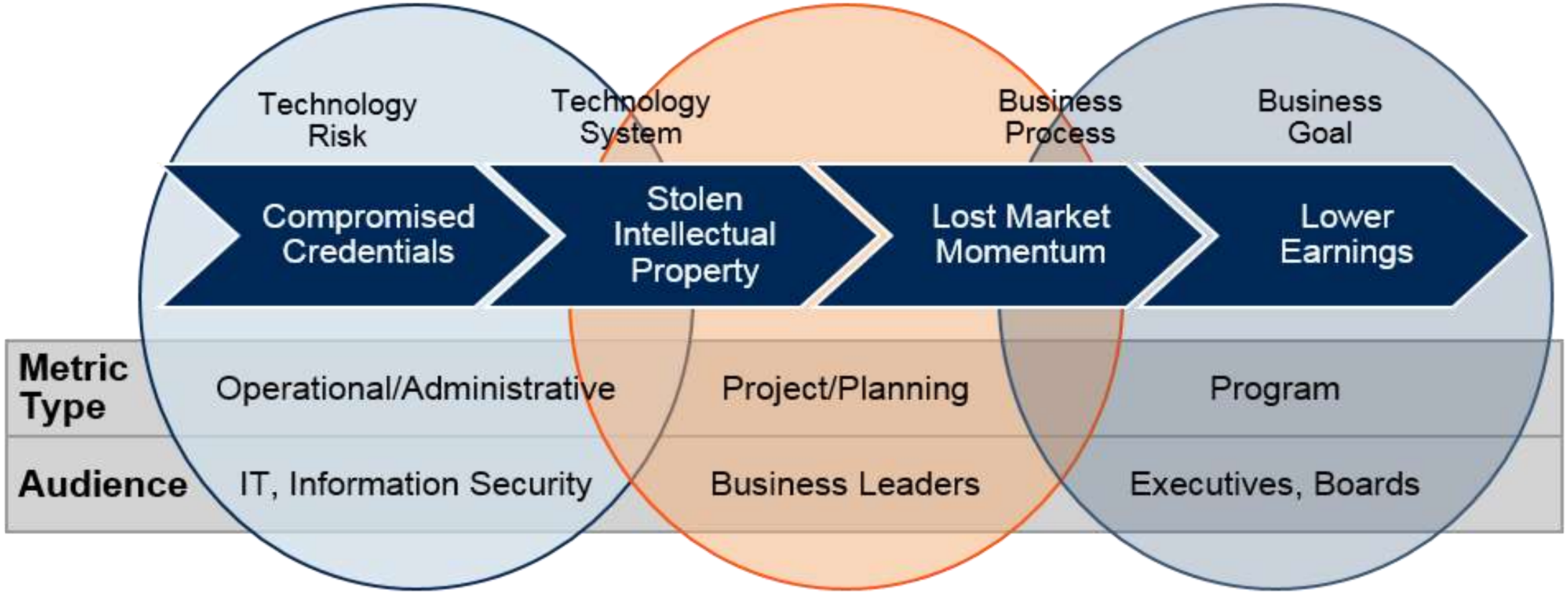
Gartner

The Metrics Chasm

Gartner

Who Cares About What?

Types of Security Metrics



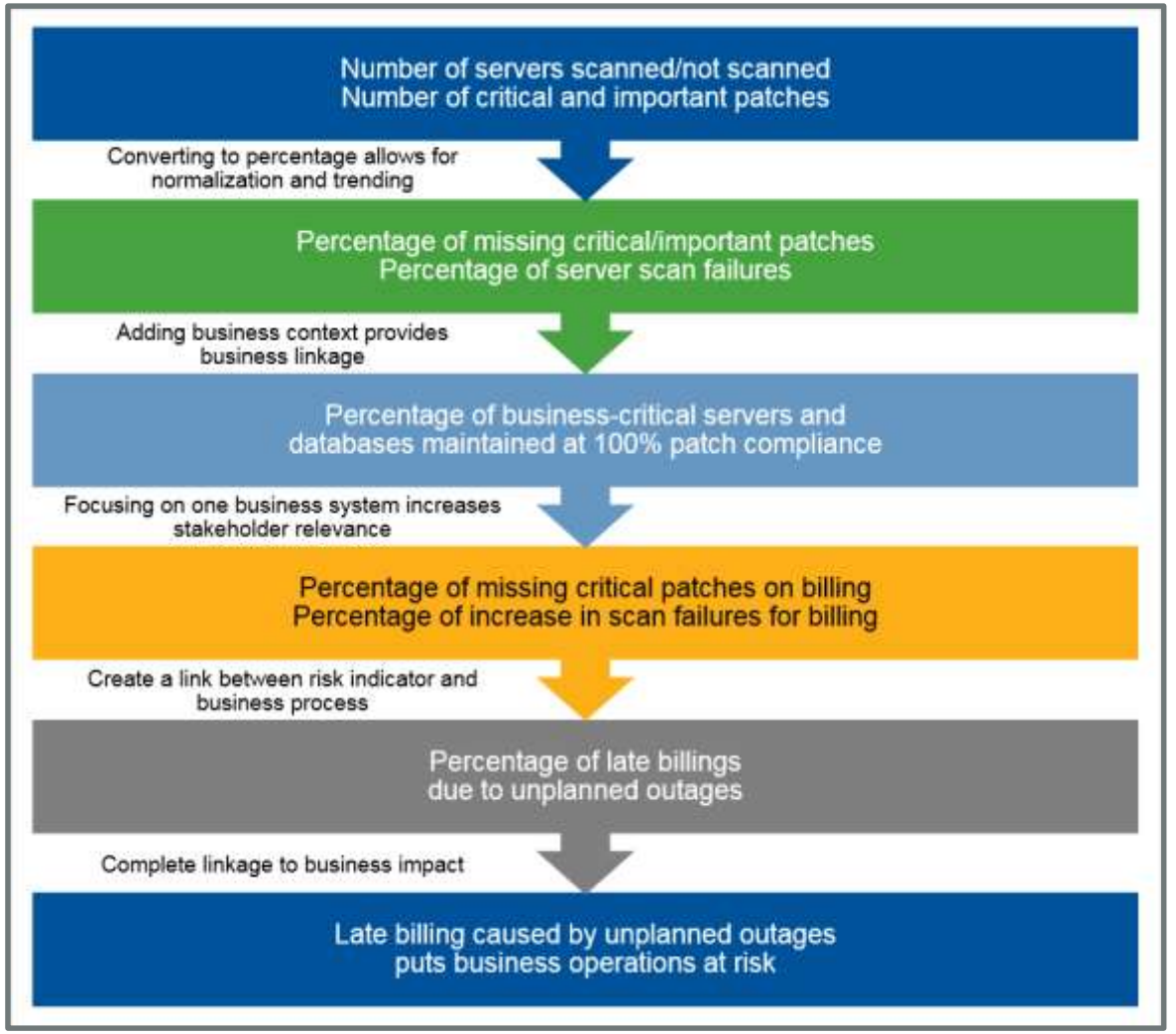
Gartner

Gartner's Business Value Model

Business Aspect	Aggregates	Primes			
Demand Management	Market Responsiveness	Target Market Index	Market Coverage Index	Market Share Index	Opportunity/ Threat Index
		Product Portfolio Index	Channel Profitability Index	Configurability Index	
	Sales Effectiveness	Sales Opportunity Index	Sales Cycle Index	Sales Close Index	Sales Price Index
		Cost-of-Sales Index	Forecast Accuracy	Customer Retention Index	
	Product Development Effectiveness	New Product Index	Feature Function Index	Time-to-Market Index	R&D Success Index
Supply Management	Customer Responsiveness	On-Time Delivery	Order Fill Rate	Material Quality	Service Accuracy
		Service Performance	Customer Care Performance	Agreement Effectiveness	Transformation Ratio
	Supplier Effectiveness	Supplier On-Time Delivery	Supplier Order Fill Rate	Supplier Material Quality	Supplier Service Accuracy
		Supplier Service Performance	Supplier Care Performance	Supplier Agreement Effectiveness	Supplier Transformation Ratio
	Operational Efficiency	Cash-to-Cash Cycle Time	Conversion Cost	Asset Utilization	Sigma Value
Support Services	Human Resources Responsiveness	Recruitment Effectiveness Index	Benefits Administration Index	Skill Inventory Index	Employee Training Index
		HR Advisory Index	HR Total Cost Index		
	Information Technology Responsiveness	System Performance	IT Support Performance	Partnership Ratio	Service-Level Effectiveness
		New Project Index	Cost Index		
	Finance and Regulatory Responsiveness	Compliance Index	Accuracy Index	Advisory Index	Cost-of-Service Index

Gartner

Context Is Key



Gartner

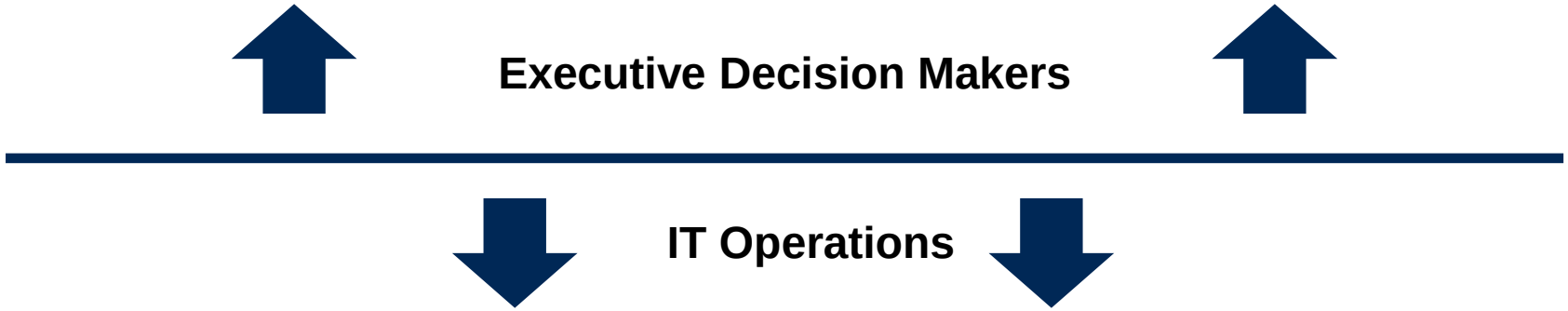
Key Issues

1. What are the characteristics of an advanced KRI?
2. How can I create leading indicators with defensible causal relationships to business impact?
3. What are some real-world examples of creating advanced KRIs?

Criteria for Good Key Risk Indicators

- Has a clearly defined and defensible causal relationship to a business outcome
- Works as a leading indicator of risk
- Addresses a specific, defined audience
- Addresses business decision making for the intended audience
- Understandable by a non-IT audience
- They use indexes that fluctuate and support action

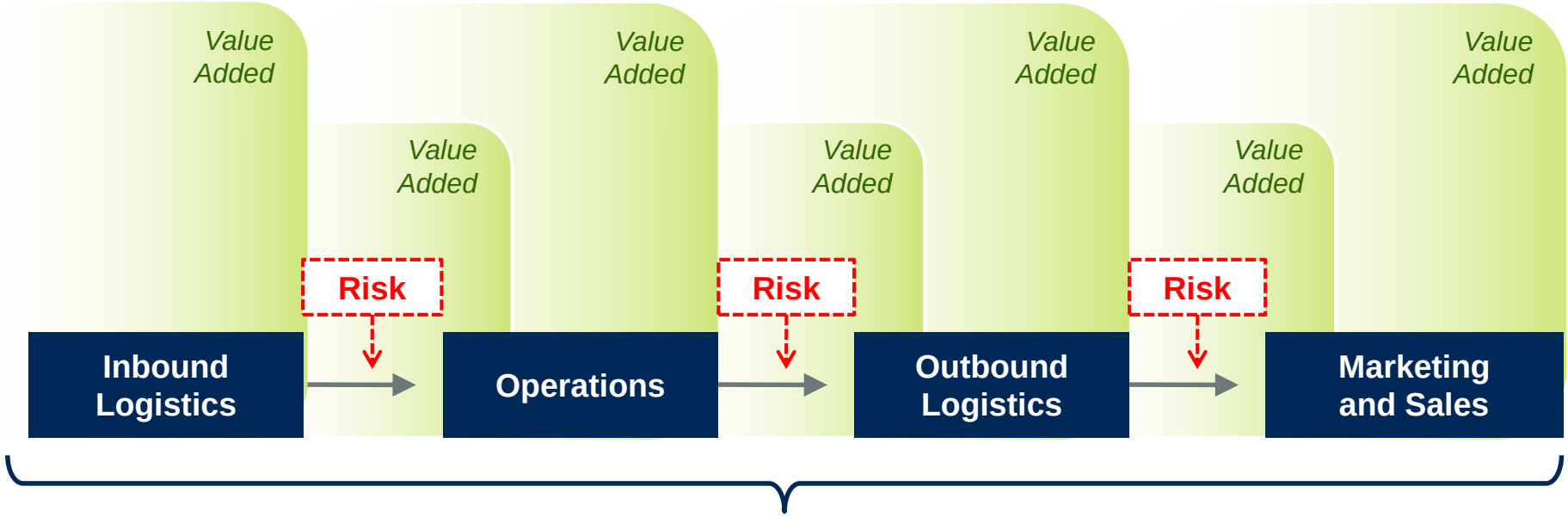
Effective Communication With Non-IT Executive Decision Makers



Operational metrics to benefit operational efficiency:

- Percentage of YTD spending of security budget
- Percentage of completion of annual objectives
- Percentage of confidence of completing objectives
- Number of new processes created and implemented
- Project status (major, per project)
- Percentage completed
- Percentage of confidence of completion
- Number of compliance deficiencies, last audit
- Number of remaining open compliance deficiencies

Risk-Adjusted Value Management

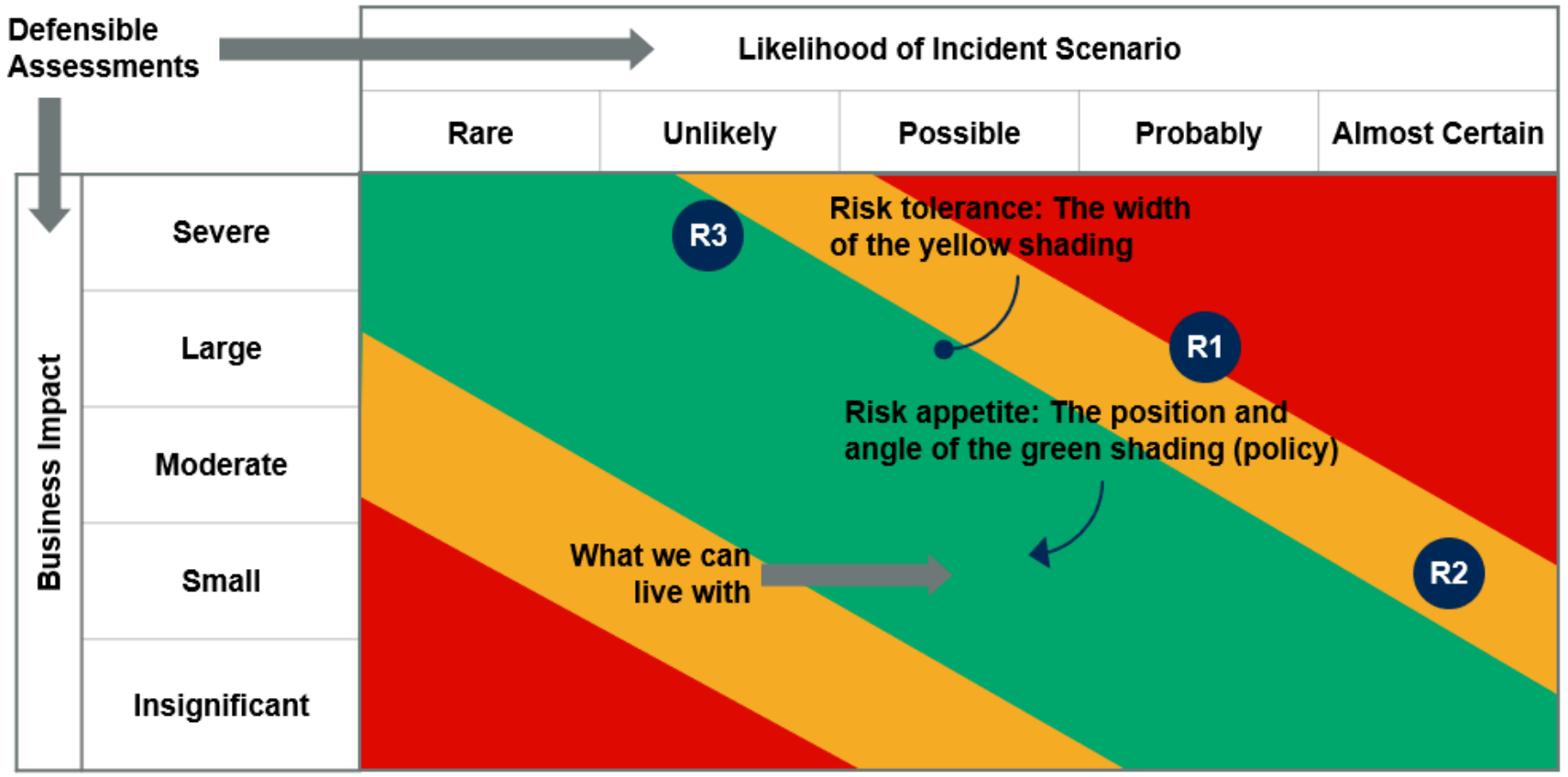


Value Chain Example (Michael Porter)

Risks are often ignored in traditional value management, Addressing them can add new value.

Gartner

Risk-Based View for the Board



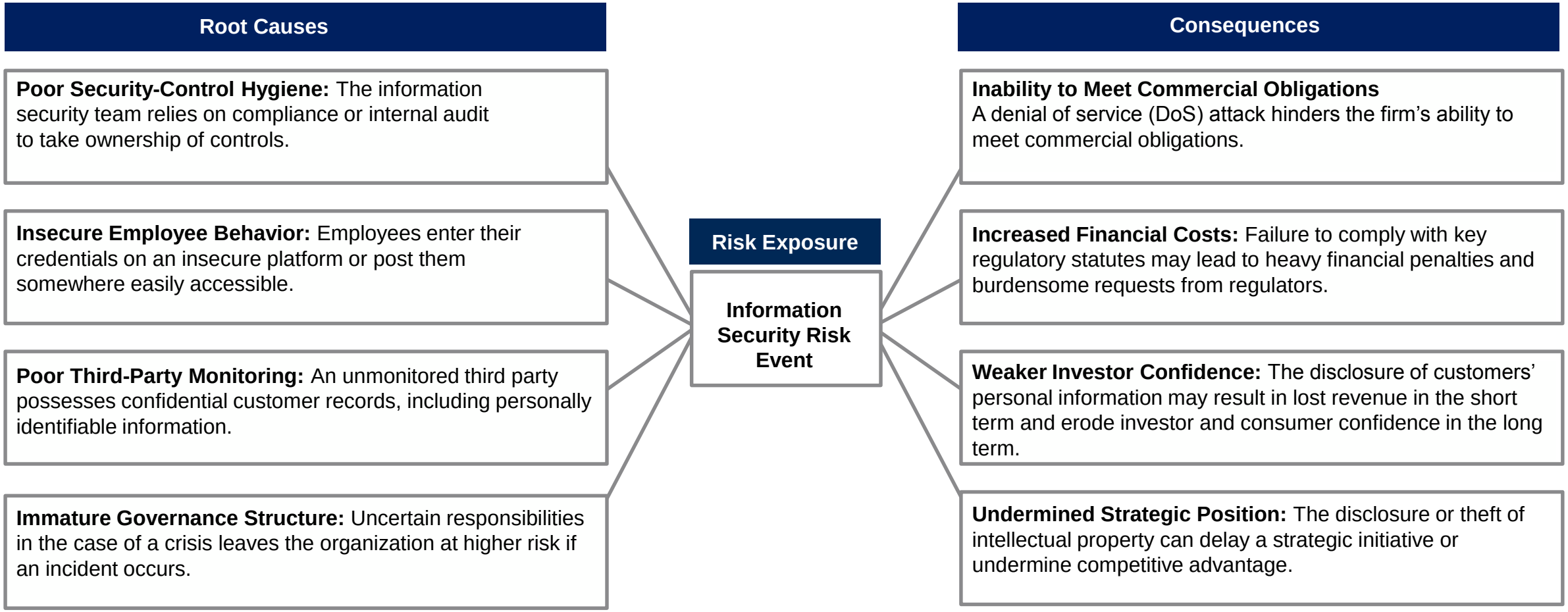
R1	Loss of product and manufacturing secrets due to disclosure of sensitive intellectual property
R2	Loss of consumer confidence and sales due to audit failure
R3	Degradation of production volume due to manufacturing interruption

Casual Chain

Gartner

Understand Causes and Consequences

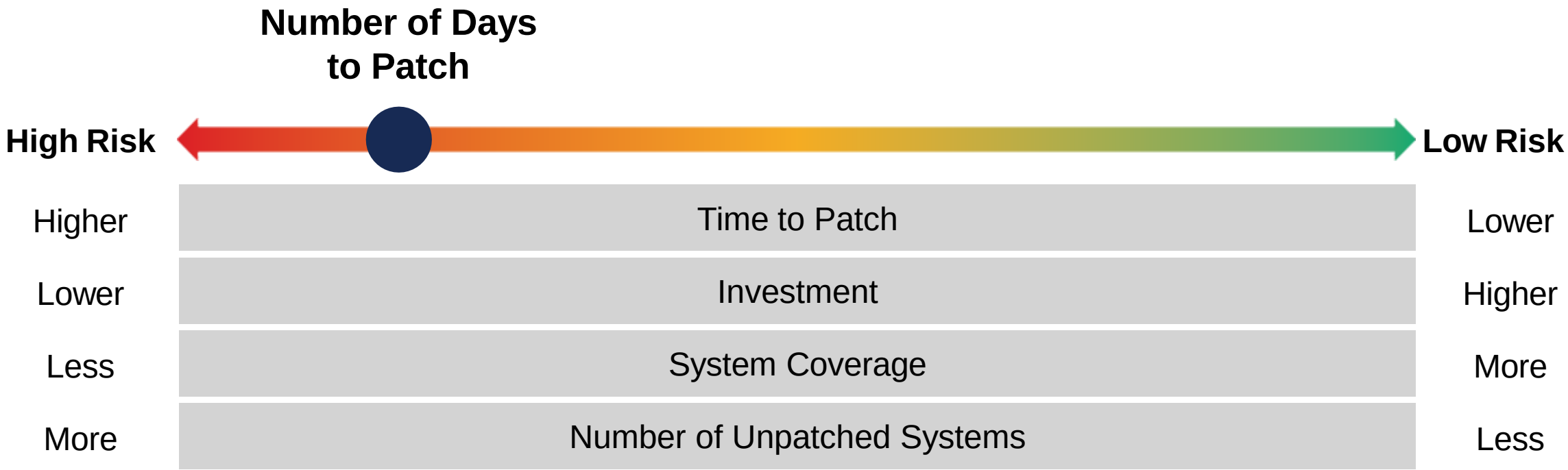
Sample Bow-Tie Diagram
(Illustrative)



Source: Gartner

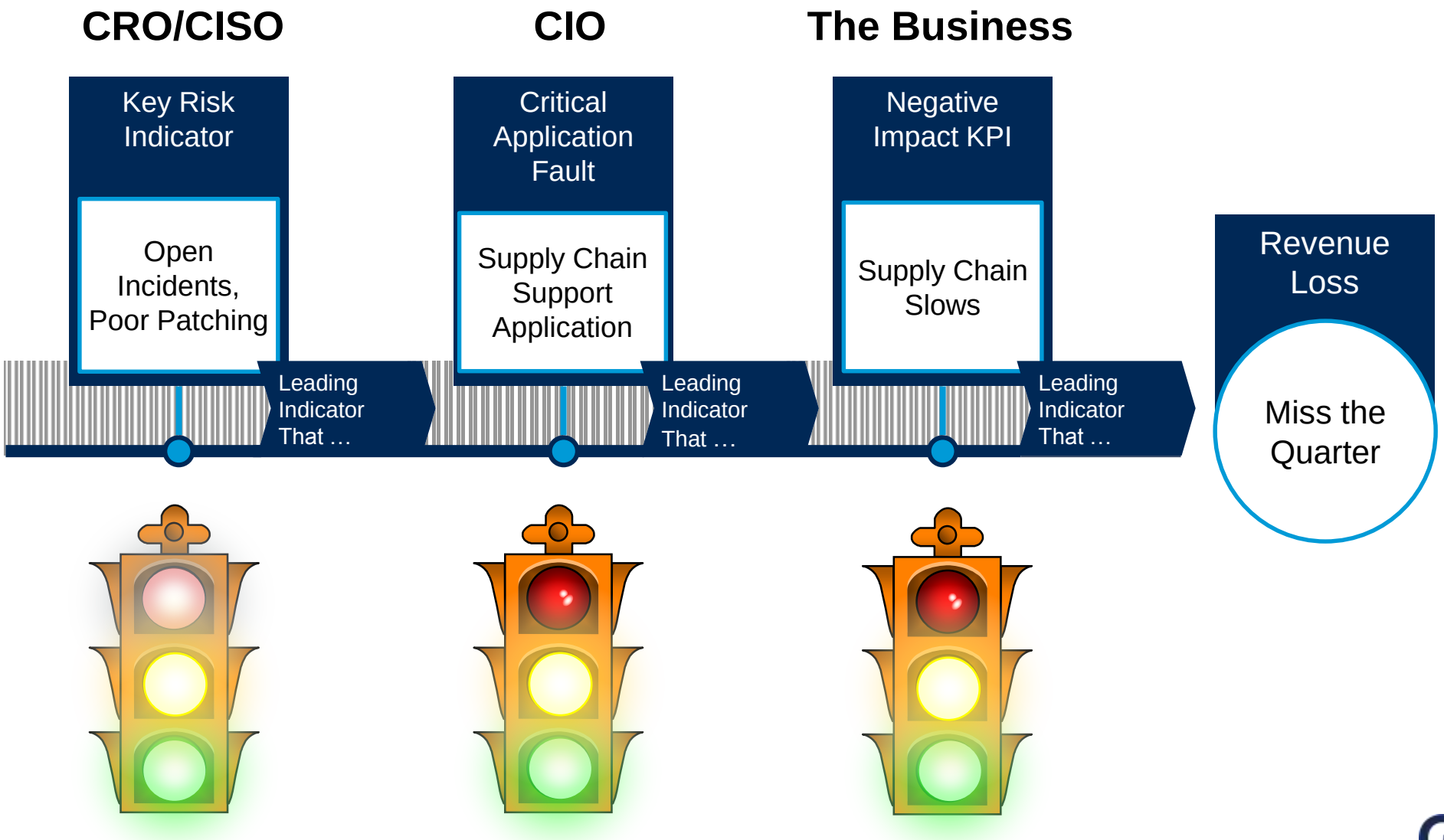
Gartner

Outcome-Driven Metric



Source: Gartner

Mapping KRIs and KPIs



From Information to Action

Source: Gartner

Evolution of a Metric

- Number of times we were “attacked” last month:
  - Very common, almost worthless.
- Number of unpatched vulnerabilities:
  - Very common. Potential, but not specific enough to guide even operational decision making.
  - Improvement only demonstrates that you are doing your job.
- Number of unpatched critical vulnerabilities against critical systems:
  - Not as common as you think because most organizations don't know which systems are critical.
  - Potential for useful operational decision making, but a “number” can be meaningless.

Evolution of a Metric (continued)

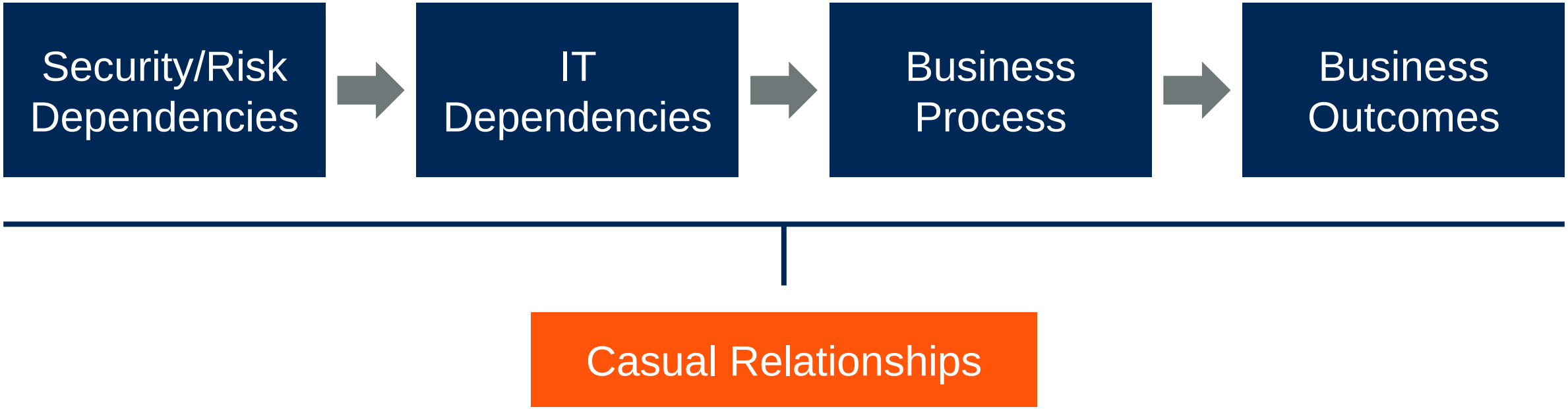
- Percentage of unpatched critical vulnerabilities against critical systems:
  - By normalizing the number we can compare it month over month.
  - Useful for operational decision making to guide resources.
  - Still worthless for executive decision makers.
- Number of days it takes to patch critical systems with critical patches:
  - Abstracts out the technology so it is understandable by a non-IT decision maker.
  - Still not useful for non-IT decision making because it has no business context.

Evolution of a Metric (continued)

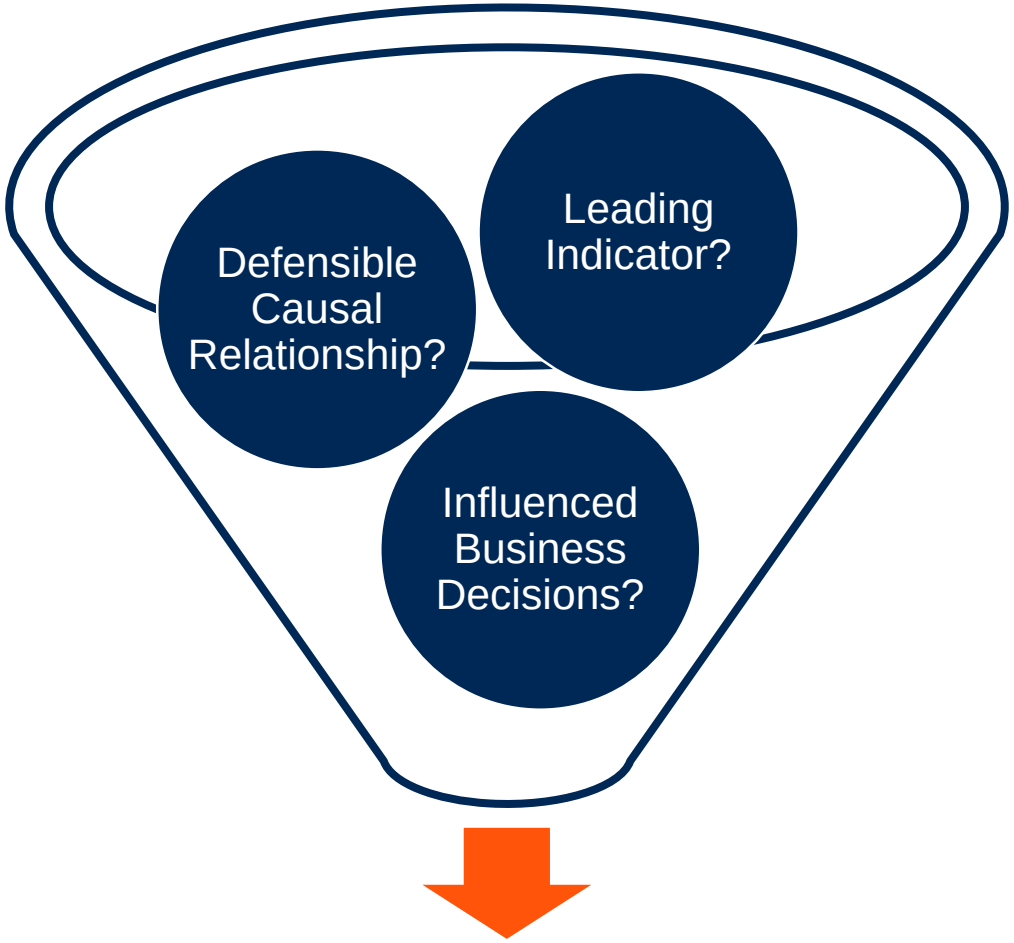
Number of days it takes to patch systems supporting the manufacturing line in Kuala Lumpur with critical patches:

- Context:
  - The manufacturing line in Kuala Lumpur has 3x the unscheduled outage time caused by IT of all the other facilities.
  - It represents 40% of the company's revenue based on new contracts in the last year.
- Reporting this to the CIO and the P&L business owner helps them:
  - Address the unscheduled outage time.
  - Address a very upset CEO who wants to know why output dropped 3% last quarter at the most critical business line.
- This is a useful above-the-line metric because:
  - The technology is abstracted out.
  - It has a business context.
  - It supports critical decision making all the way up to the CEO.

Create Your Own Value Chain



Remember the Litmus Test



A Useful Metric

Gartner

Recommendations

- Review all of your dashboards and metrics.
- Define the audience they address.
- Determine the decisions for the audience that are influenced by the metrics.
- Determine the causal relationships each metric has to a business dependency.
- Revise your metrics to be leading indicators.
- Reposition IT operational metrics away from business decision makers.

Recommended Gartner Research

- **Toolkit: Board-Ready Slides for Cybersecurity and Technology Risk**
  Rob McMillan, Paul Proctor and Jeffrey Wheatman (G00328469)
- **Develop Key Risk Indicators and Security Metrics That Influence Business Decision Making**
  Paul Proctor, Jeffrey Wheatman and Others (G00366666)
- **Outcome-Driven Metrics for Cybersecurity in the Digital Era**
  Paul Proctor (G00466057)
- **Five Board Questions That Security and Risk Leaders Must Be Prepared to Answer**
  Sam Olyaei and Jeffrey Wheatman (G00377323)