Managing Cyber Risk as a Strategic Enterprise Risk

John Button, M.A., RIMS-CRMP, OpenFAIR
Principal, Enterprise Risk Management

FAIR22 CONFERENCE

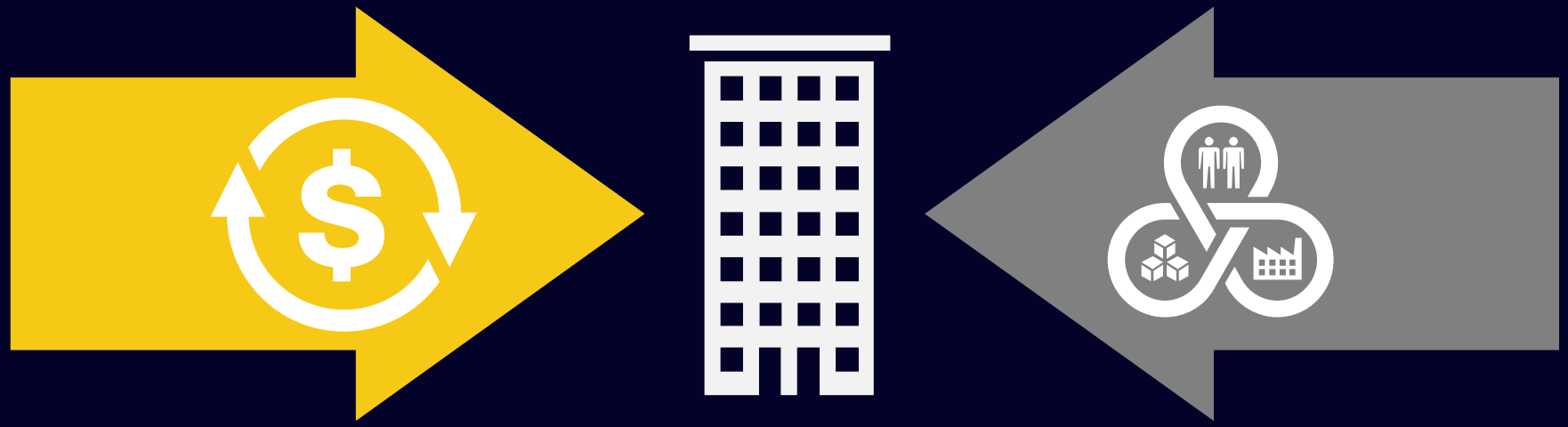
Roadmap

FAIR22 CONFERENCE

Roadmap

FAIR22 CONFERENCE

2022 – 2023 Economic Landscape



Global Economic Uncertainty

Next Wave of Digital Expansion

FAIR22 CONFERENCE

Acceleration of Digital Initiatives

69%

of BoDs cite **acceleration of digital initiatives** as an impact of COVID-19

64%

of organizations are **accelerating** their **digital investments**

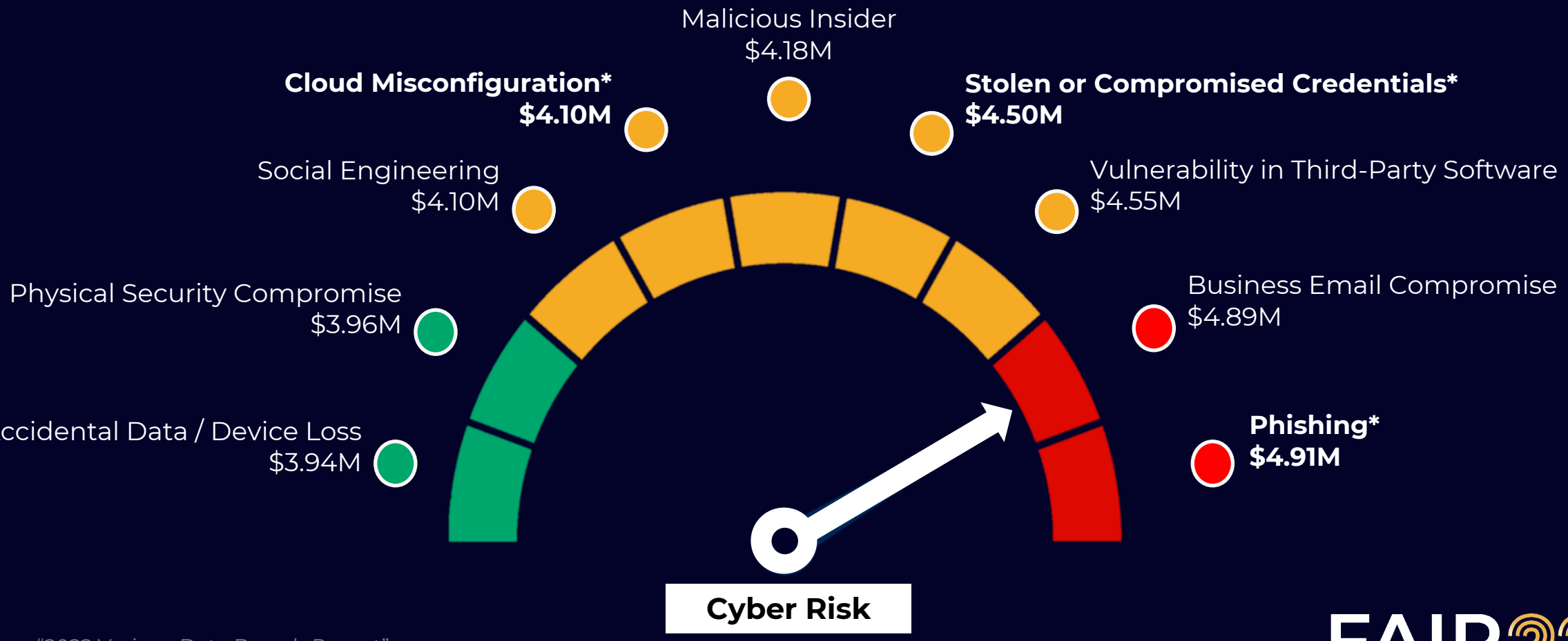
83%

of CEOs are looking to **increase** their **investment** in **digital capabilities**

FAIR22 CONFERENCE

Cyber Risk is at an All-Time High

Average cost and frequency of data breaches by initial attack vector



Sources: "2022 Verizon Data Breach Report"

FAIR22 CONFERENCE

Global Attack Surface Growing Faster Than You Think

Global Attack Surface: Total set of cybersecurity exposures across all your organization's systems, networks, and the exposure of third parties. This includes everyone in the enterprise "ecosystem" including major customers, vendors, and perhaps government agencies.

Reason for increasing attack breaches and anticipated breaches:

- Increasing number of persons on the internet
- Number of uses per person for online resources (includes IoT)
- Each user spends more time online and gets more services and products online
- Vulnerabilities continue to increase
- Major breach cascading

The Global Attack Surface Grows Every Minute

117,289 hosts created each minute.

613 domains created each minute.

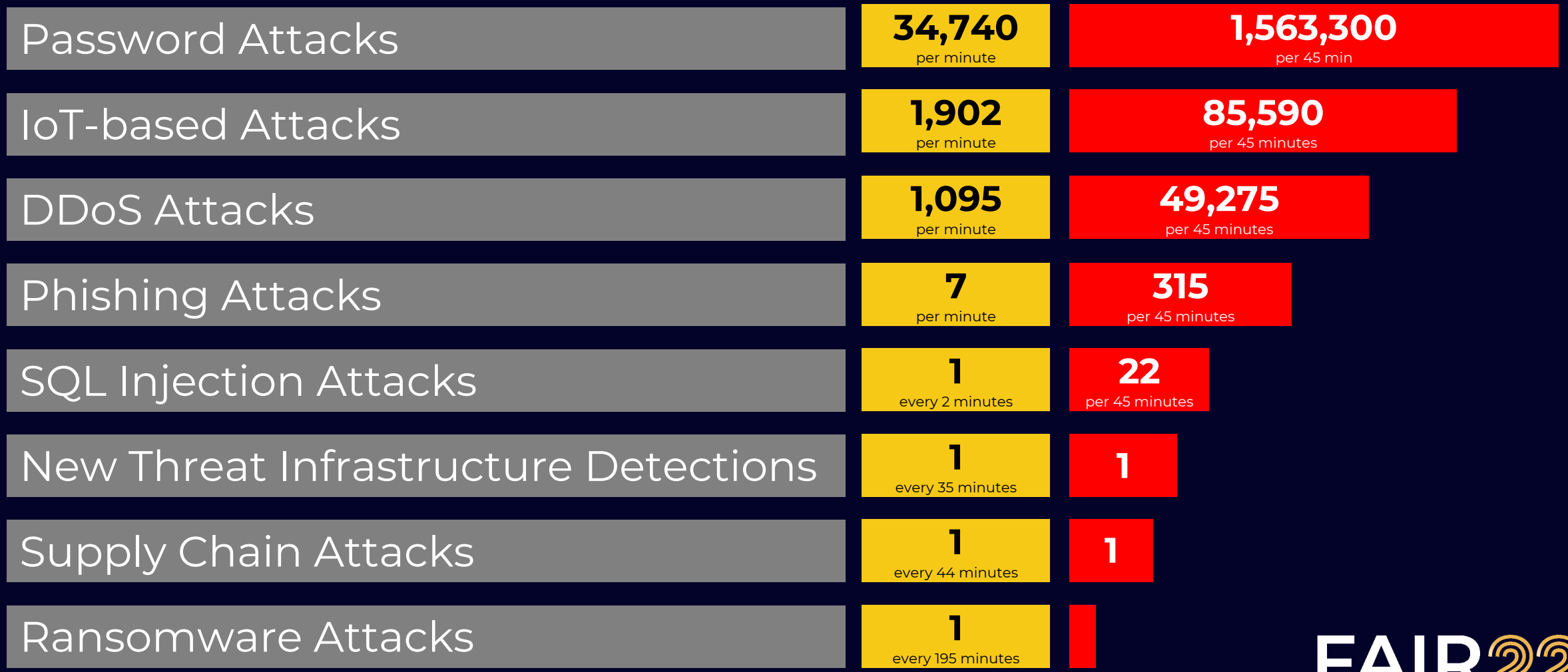
375 new threats each minute

Source "How to Measure Anything in Cybersecurity," Doug Hubbard; Microsoft, "The global attack surface may be bigger than most think" April 2022

FAIR22 CONFERENCE

The Scale and Scope of Worldwide Cybercrime

In any given 60-second window, the following malicious activity is happening.



FAIR22 CONFERENCE

New Key Drivers of 2022 Enterprise Cyber Risk

NEW DRIVERS

Increasing Risk Appetite
57% of Boards have increased or expect to increase their cyber risk appetite

Talent Shortage
The global cyber workforce needs to grow 65% to defend organizations' critical assets.

Shifting Investments
Digital technology initiatives rank as the top business priority for boards & CEOs

Distributed Decisions
More risk decisions, of more types, by more people, are made outside of IT or InfoSec.

3rd-Party Vulnerabilities
the overall economic structure to a more digital economic architecture

Threat Sophistication
A vicious cycle ensues; as our defenses get stronger, attackers get more sophisticated.

Growing Attack Surface
The global attack surface is rapidly growing every minute, and we are all connected.

Insecure Behavior
82% of breaches in 2021 involved the human element

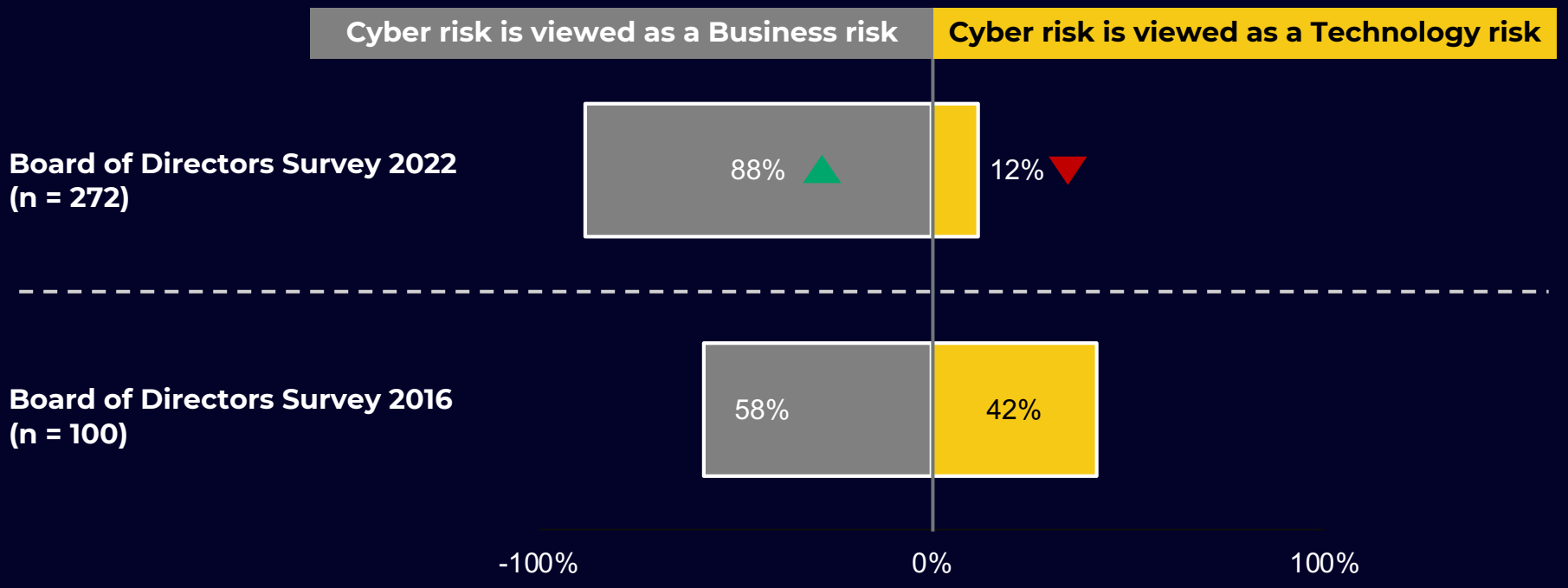
OLD-FAITHFUL DRIVERS

FAIR22 CONFERENCE

Roadmap

FAIR22 CONFERENCE

Cyber Risk Viewed as a Business Risk



▲▼ High/low significance differences between 2022 vs. 2016 survey

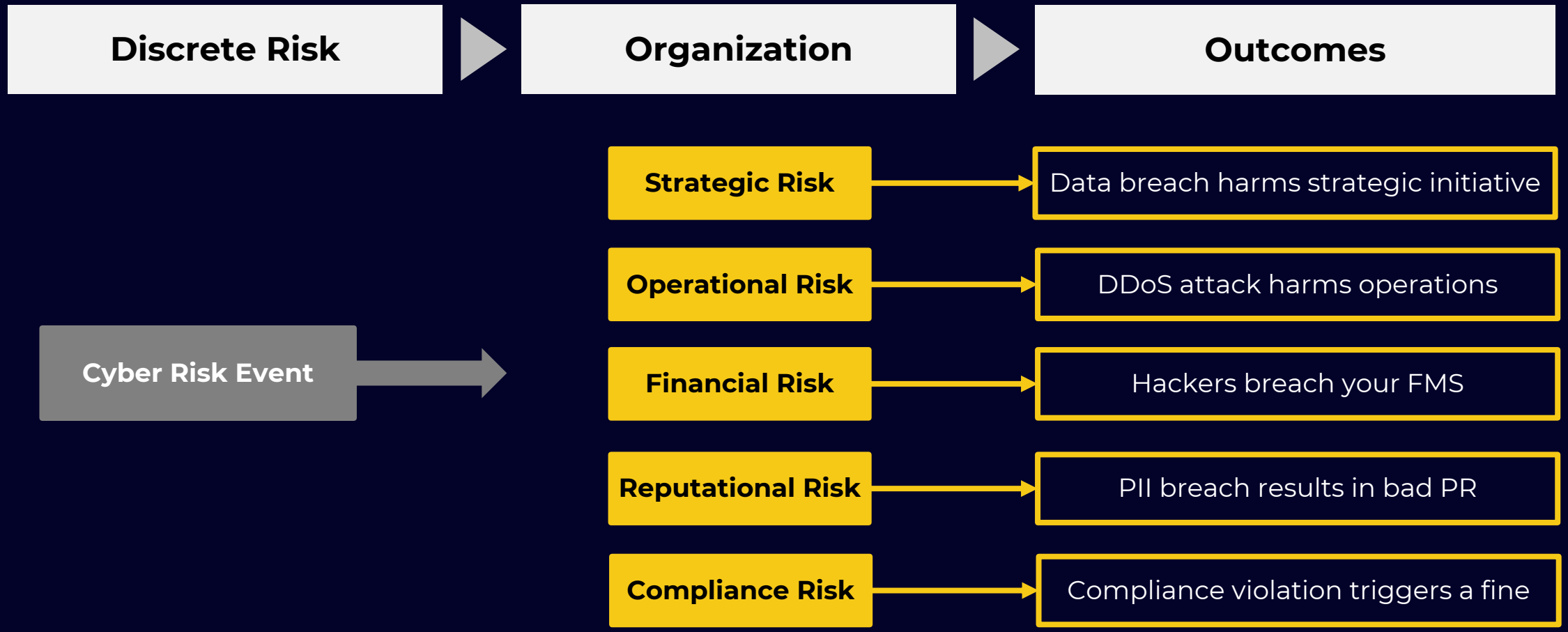
n varies ; All Respondents, Excluding Don't Know

Q07. Please tell us which of the two opposing viewpoints most closely represents how cyber-security is viewed and handled in your organization.

Source: 2022 Gartner View from the board of Directors' Survey

FAIR22 CONFERENCE

Cyber Risk Impacts the Organization



Enterprise Impact of Cybersecurity Regulations

NYDFS Proposes Significant Changes to its Cybersecurity Rules (23 NYCRR 500) and requires an enterprise view:

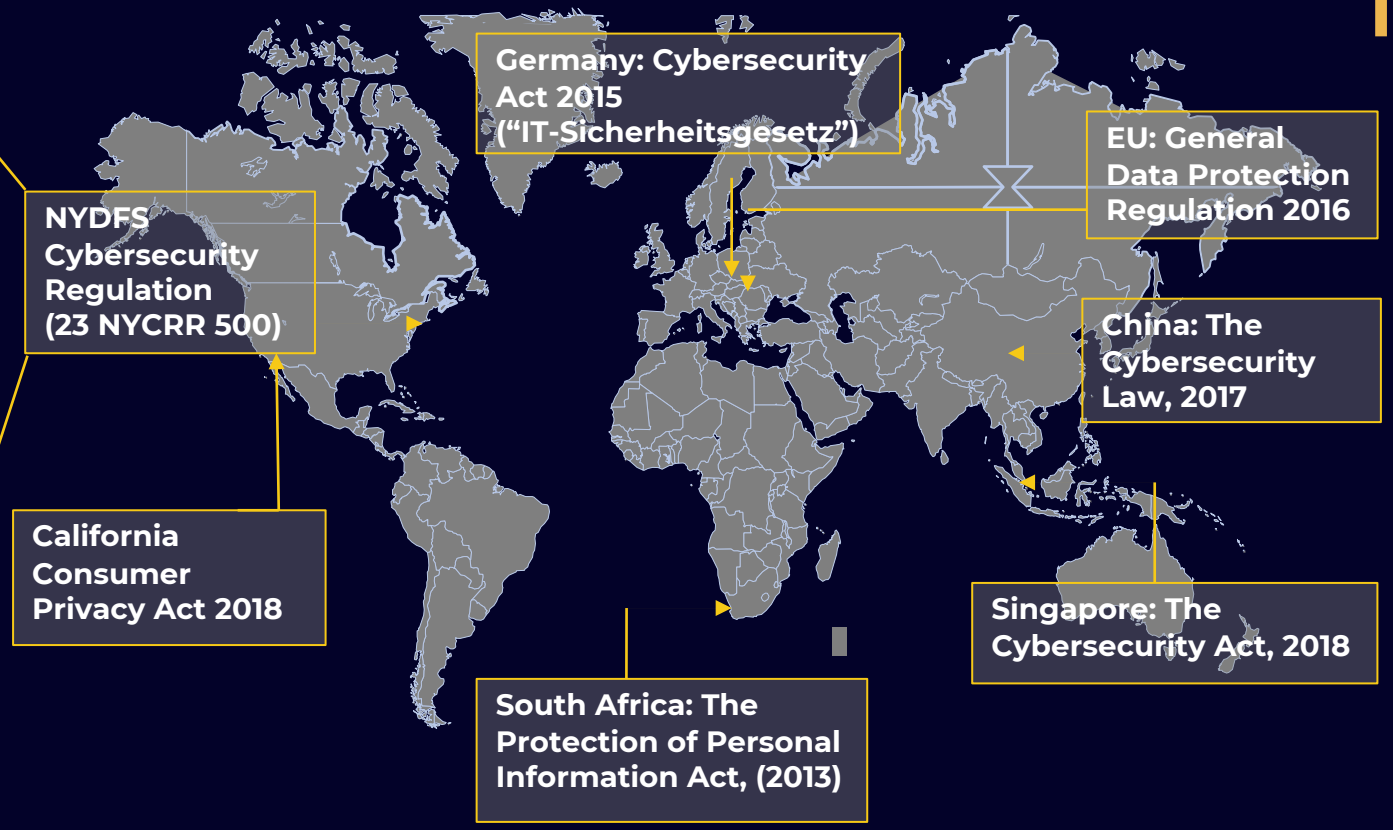
72-Hour Notice of ransomware events that result in a material part of the covered entity's information system.

CEO certification: The annual certification of compliance must be signed by the CEO and the CISO (rather than by a Senior Officer).

Executive Mgmt Involvement: Board must delegate the development, implementation, and maintenance of the infoSec program to the executive management (or its delegates).

Questions ERM will be integral in answering:

- How could a cyber compliance failure **impact our reputation?**
- Is **CRM fully integrated** into our ERM process, and is our process effective?
- Should we transfer risk via **D&O insurance** for the CISO? Additional insurance for executive management?



Sources: Gartner; "GDPR Compliance Solutions for Cyber Security" Huntsman; "China's Cybersecurity Law: What You Need to Know" The Diplomat; "The Singapore Cybersecurity Act 2018" Simmons+Simmons; "Cybersecurity Compliance: A Comprehensive Guide" darkcubed; "Cybersecurity in Germany" Simmons+Simmons.

FAIR22 CONFERENCE

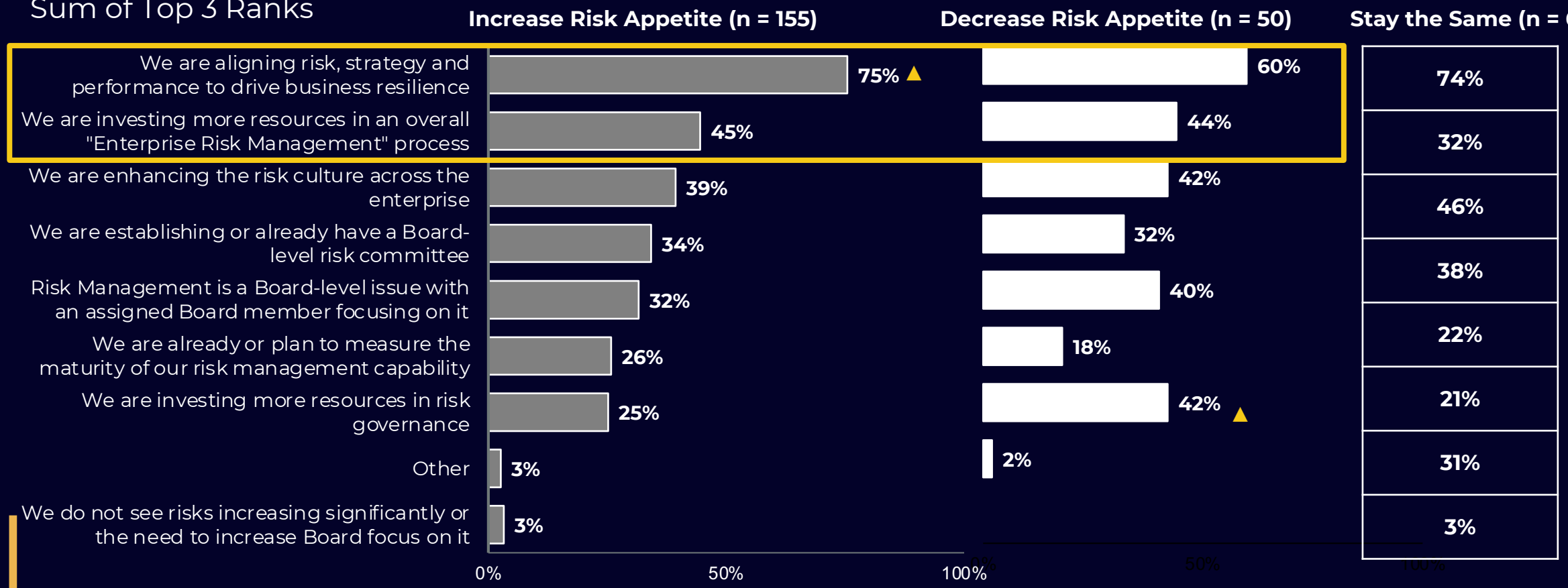
FAIR22 CONFERENCE

The Puzzle to Solve

Good News: Boards View ERM as the Way Forward

Top Approaches for Handling Risks

Sum of Top 3 Ranks



n varies ; Organization's performance have/expected some performance risks (Q02) and/or some external geopolitical and/or social trends source of risk (Q03), Excluding Don't Know

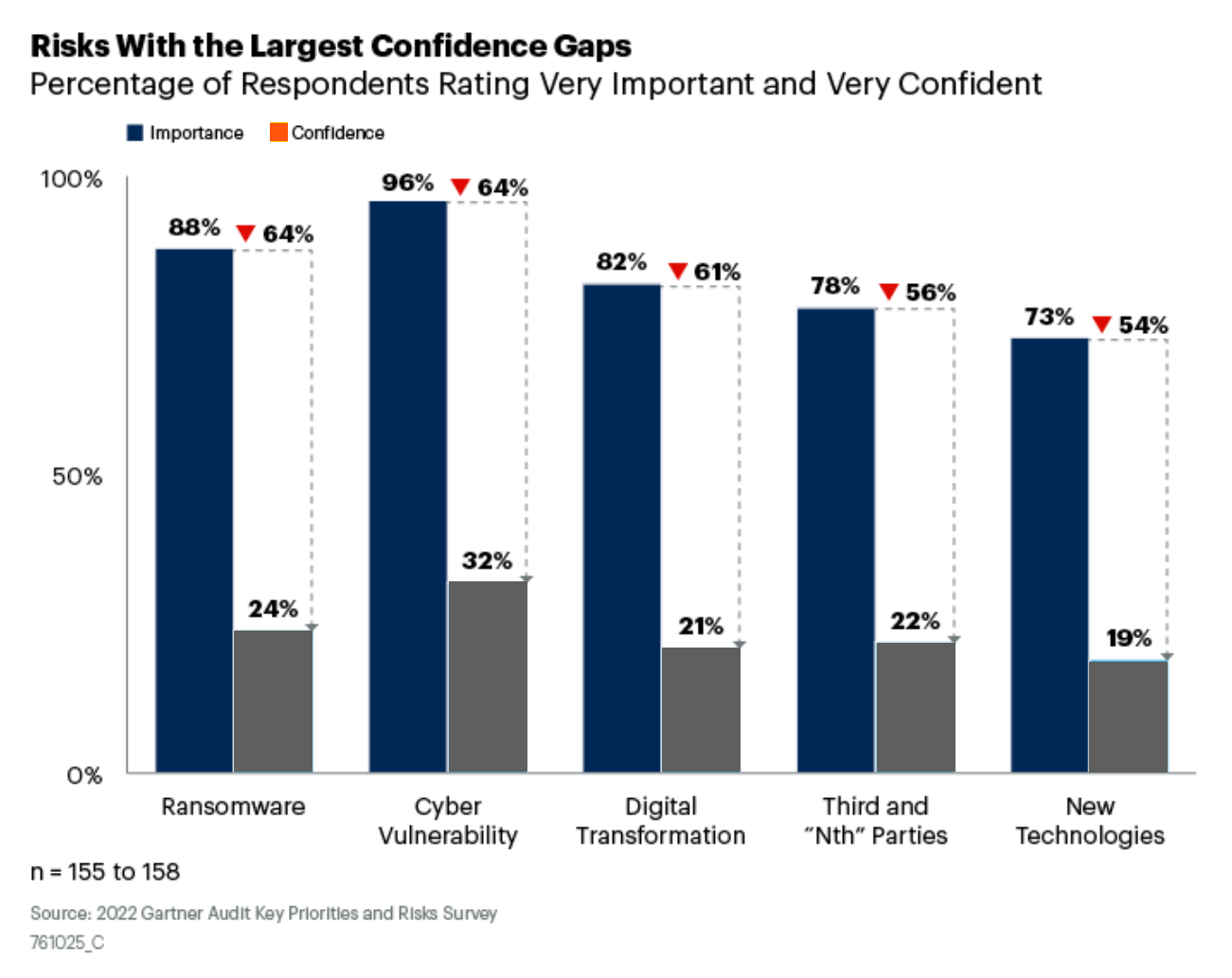
Q04. What are your top 3 approaches for handling these risks?

Source: 2022 Gartner View from the board of Directors' Survey

▲ Significant differences between organizations increasing and decreasing risk appetite

FAIR22 CONFERENCE

Bad News: Technology-Risk Confidence Gaps



- Ransomware and cyber vulnerability have the largest confidence gaps at 64 percentage points each
- Audit leaders admit 54% confidence gap for newer technologies
- Audit leaders rate cyber vulnerability (96%) and ransomware (88%) most important risks
- More sophisticated attacks lead average recovery costs to more than double over the past year
- 53% of audit leaders feel the need to address IT auditing practices failing to keep pace with technologies and IT risks

FAIR22 CONFERENCE

The Missing Piece

SRM & CISOs

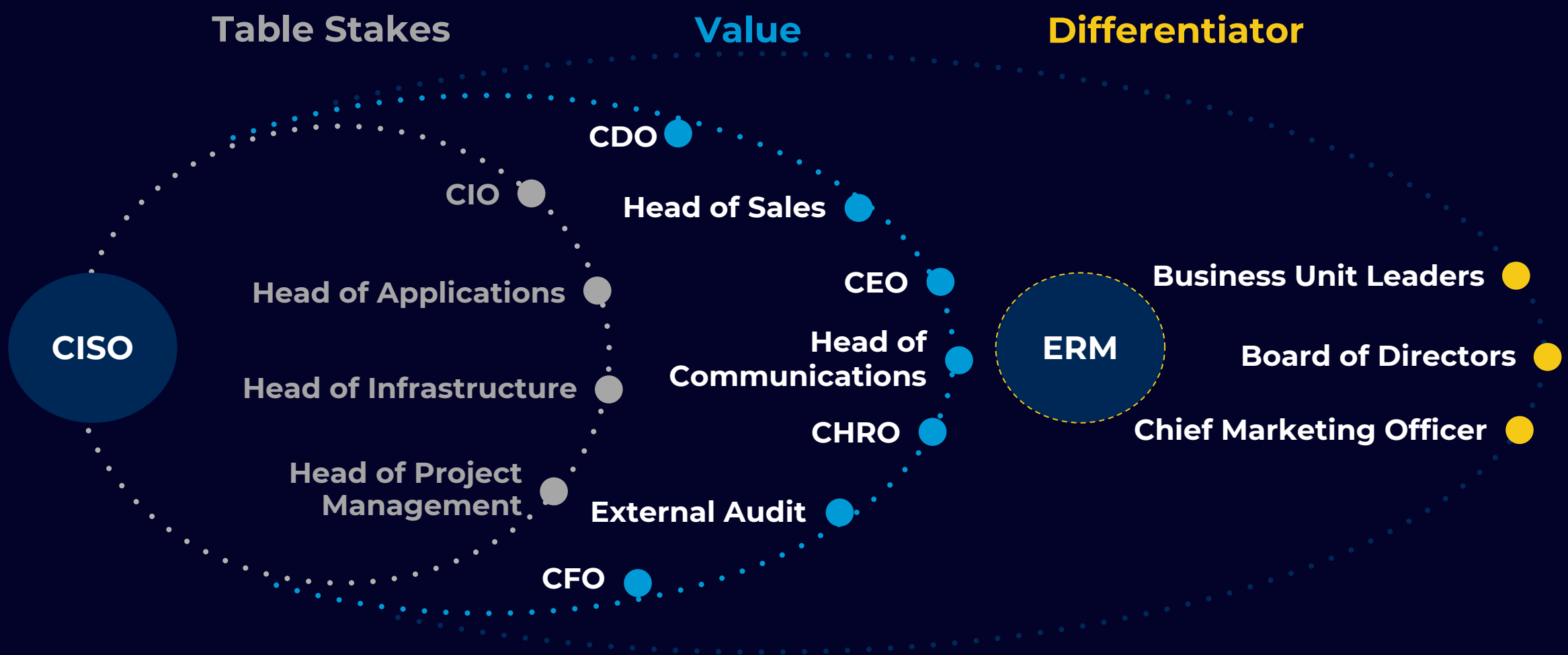
- **Limited line-of-sight** across the enterprise risk portfolio
- **Resource limitations & Risk Process Skills**
- **Strategic (Mis)Alignment** – CISOs and IT Risk teams can be overly tactical & may not be clearly aligned to the organization's goals and objectives

ERM

- **Unique enterprise-wide vantage point** can compensate for limited line-of-sight
- **ERM are getting more resources** and are **experts in the risk process** and can help augment deficient areas
- ERM is a process **effected by the board**… applied in **strategy setting** and across the enterprise,

FAIR22 CONFERENCE

Friends in High Places



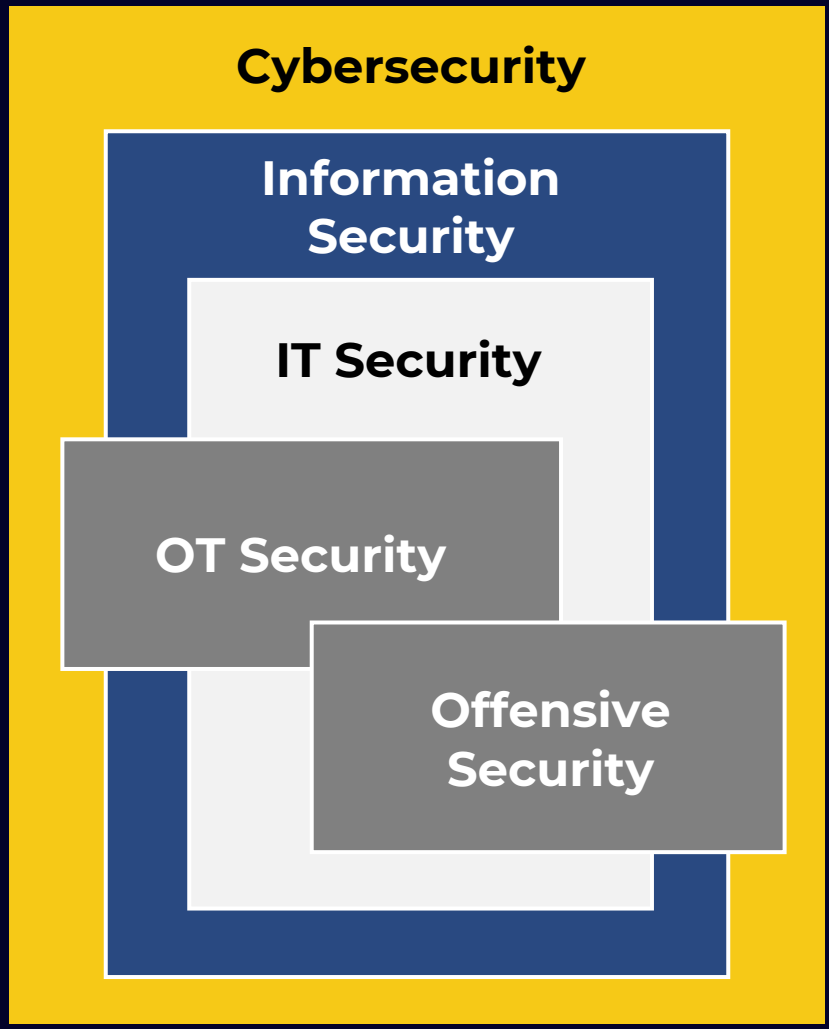
FAIR22 CONFERENCE

Roadmap

FAIR22 CONFERENCE

Enterprise Cyber Risk Management?

Enterprise Cyber Risk Management:
An integrated, thorough, and strategic approach to the measurement and management of information, systems, and asset risk across the entire enterprise.



Ensure Risk Governance: Customizable RACI

This RACI Chart Template (with prepopulated suggestions by Gartner experts) helps ERM heads create a map of people who are "Responsible, Accountable, Consulted, and Informed (RACI)" for all activities involved in managing cyber and information risk. Double-click the “Microsoft Excel Worksheet” icon to get started.

	Risk Governance			Risk Evaluation				Risk Response	
Role	**Common Risk View**	**Integrate With ERM**	**Risk-Aware Decisions**	**Provide Input**	**Collect Data**	**Analyze Risk**	**Maintain Risk Profile**	**Articulate Risk**	**Manage Risk**
Board/Senior management	A	A	C					C	
Chief executive officer (CEO)	C	R	C				C	C	A
ERM heads	R	R				C			
Chief information officer (CIO)	R	R	R	R	R	R	R	R	R
Chief information security officer (CISO)	R	R	C	R	A	A	R	A	R
Chief financial officer (CFO)	C			C					
Enterprise risk committee	C		I	C		C		R	I
Business leader	R	R	A	A	I	C	A	R	R
Business process owner	R	R	R	R	I	R	R	R	R
Compliance leader	C						I	I	

R Responsible →Those who do work to achieve the task; there can be multiple resources responsible for working on a task.

A Accountable →Those ultimately answerable for completion of the task—the task "owner;" there must be one, and only one, individual role specified for each task. Group roles should not be assigned an A.

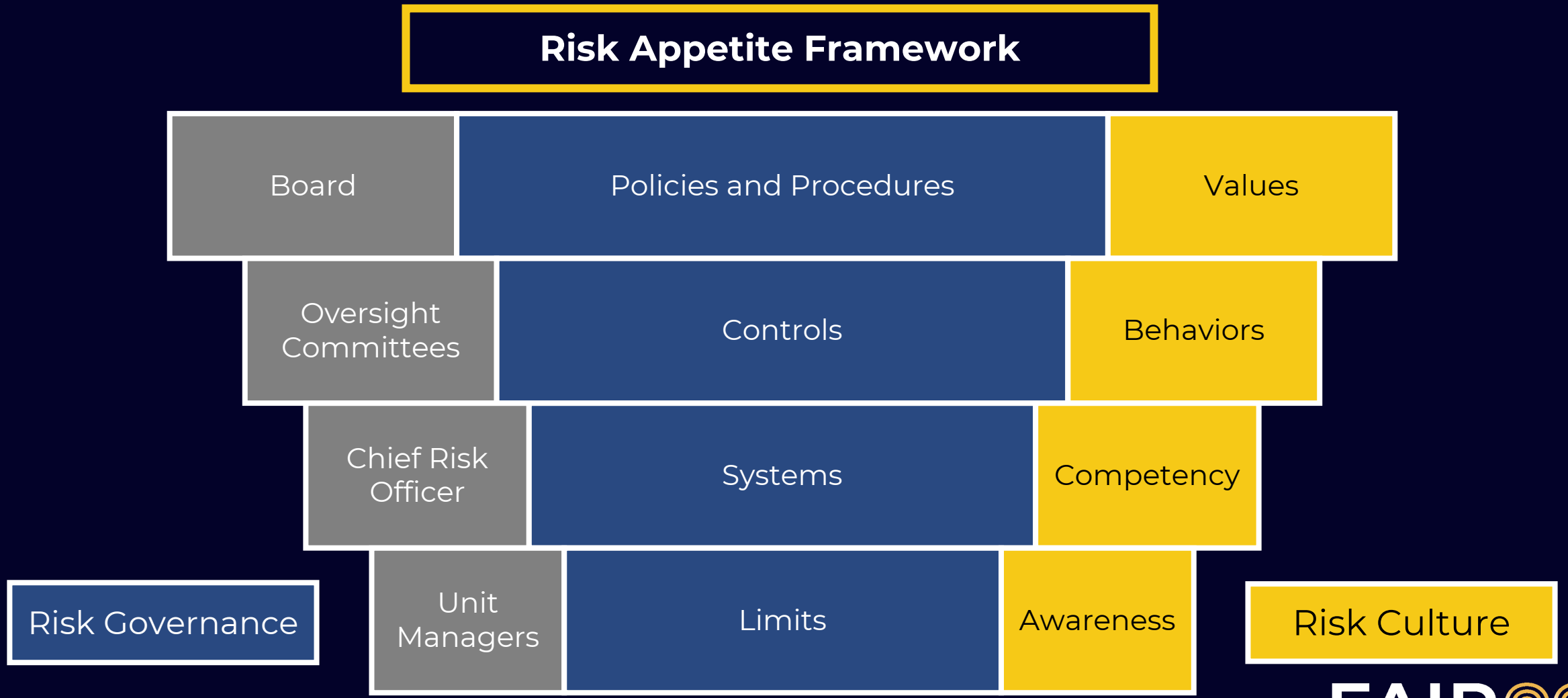
C Consulted→Those whose input/opinions are sought—two-way communication

I Informed→Those who are kept informed of progress and/or completion—typically one-way communication

Source: Gartner

FAIR 22 CONFERENCE

Align Cyber Risk, Strategy, and Performance



FAIR22 CONFERENCE

Fully Integrate CRM with ERM

NIST IR 8286A Example

1a: Enterprise Level

- Mission, strategy, priorities
- Risk Appetite Defined

1b: Org Level

- Risk appetite interpreted
- Tolerance defined (Enterprise or org level)

2a & 2b: System Level

- Application of risk strategy
- Risk assessment conducted at BU-Level
- Risk register & response recommendations updated.

4: Enterprise Level

Enterprise risk results inform:

- ERR and ERP
- Support RAS refinement,
- Improve enterprise risk decisions
- Feedback to refine risk tolerance

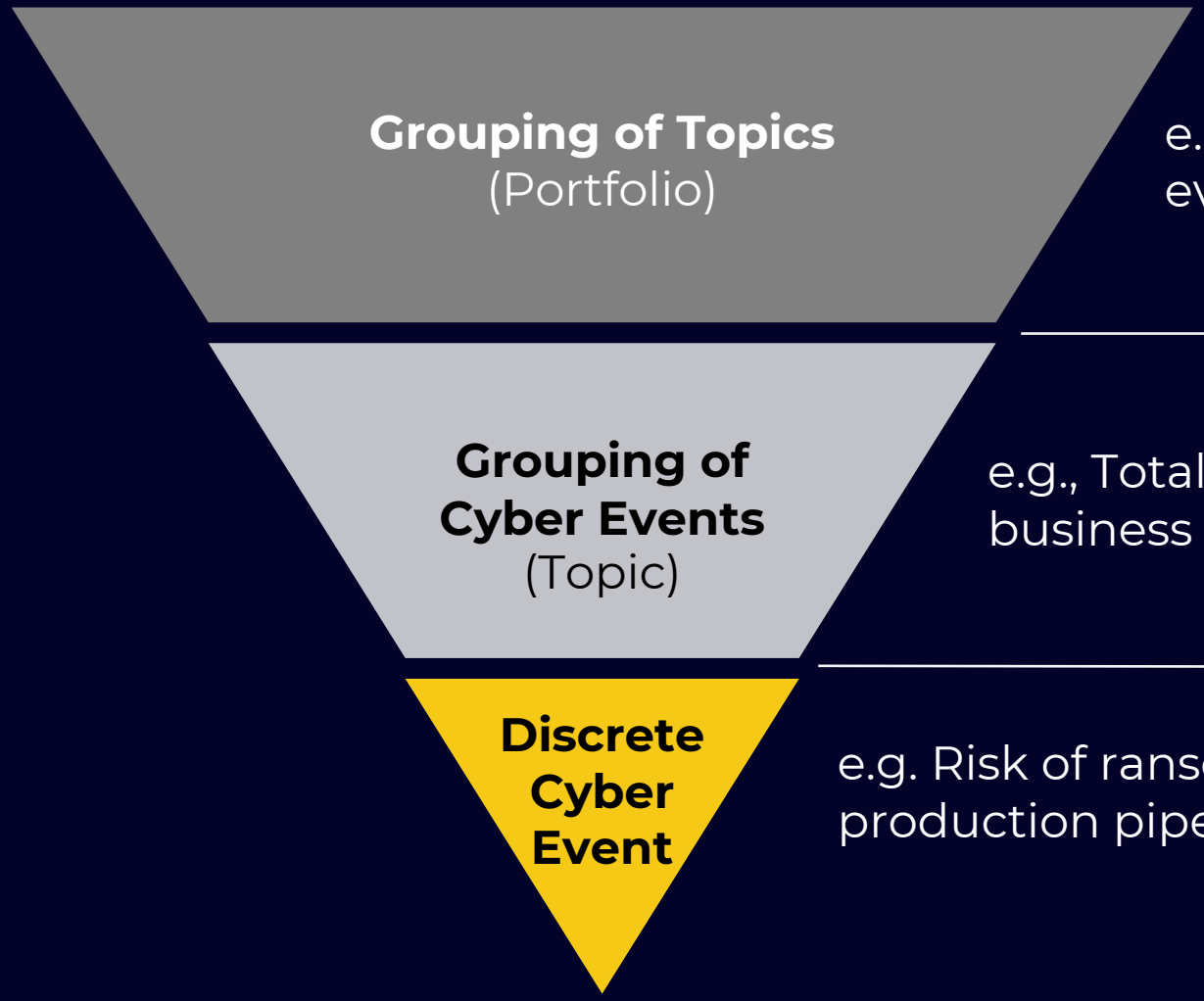
3: Org Level

- Risk Treated and residual risk reflected in System-Level CS Risk Registers
- Risk Register normalization/aggregation into Org-Level CSRRs
- Risk results reported

FAIR22 CONFERENCE

ERM Needs an Enterprise Cyber Risk Model

How do we get from the bottom to the top?



e.g., Total risk for ransomware events, across the enterprise

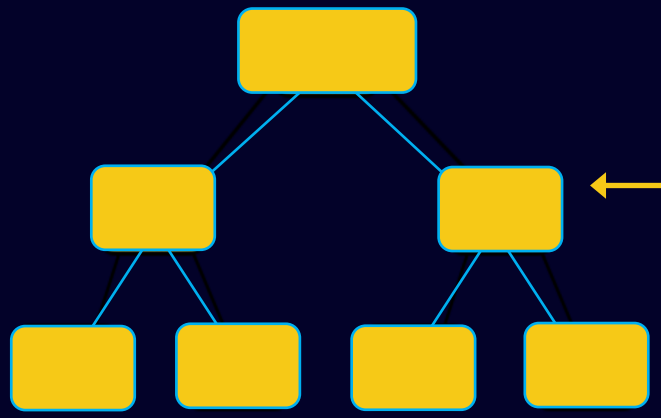
e.g., Total risk for ransomware events in business unit A

e.g. Risk of ransomware causing an outage of a production pipeline in factory A

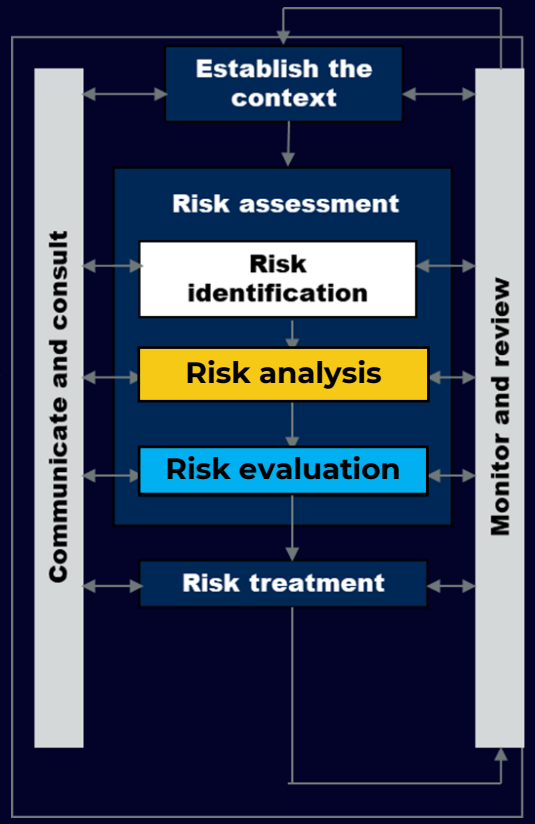
FAIR22 CONFERENCE

Adopt an Enterprise Cyber Risk & Control Model

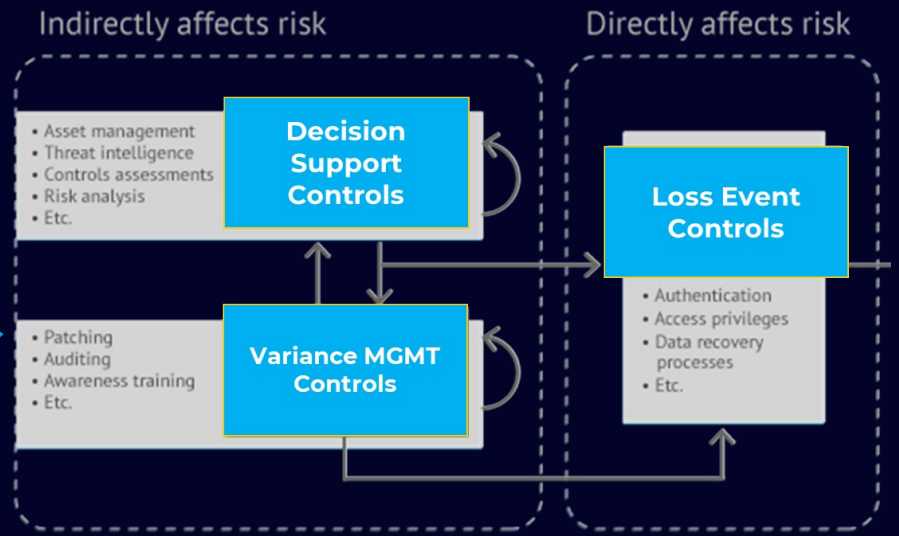
Cyber Risk Model



ISO 31000

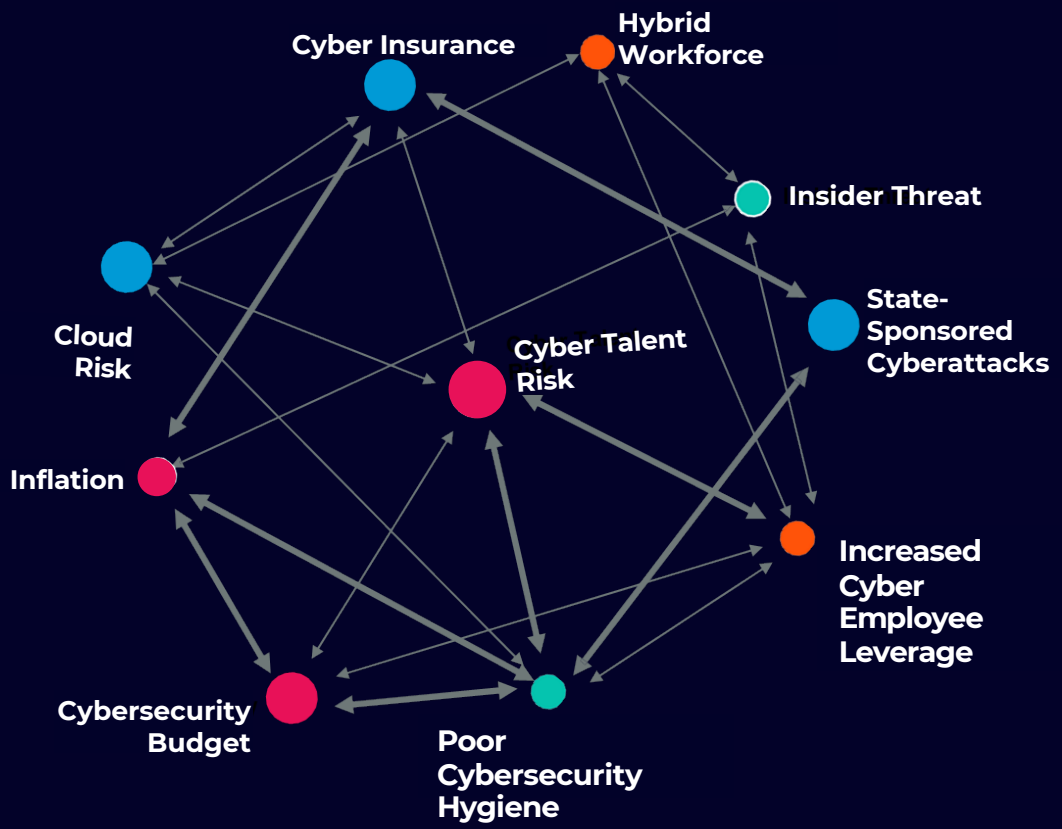


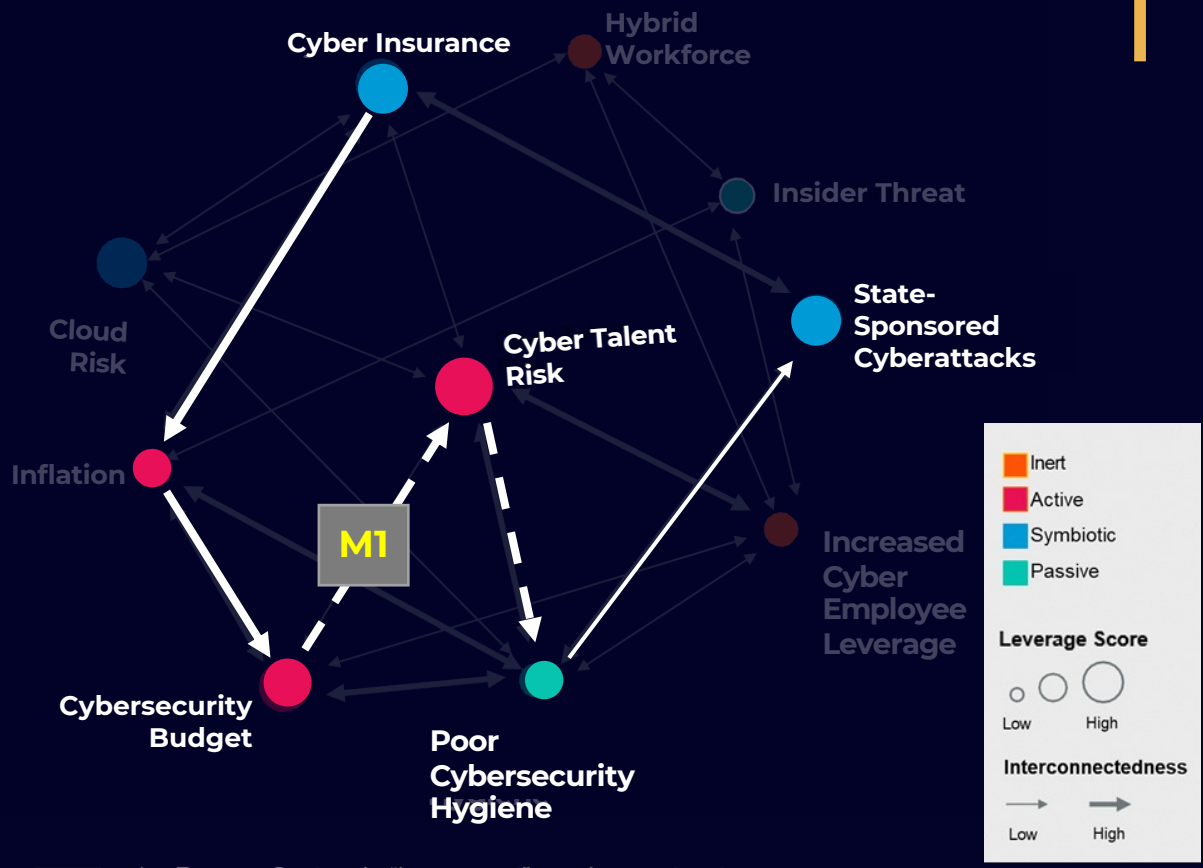
Control Analytics Model



FAIR22 CONFERENCE

Preliminary Risk Interdependency Modeling





M1

1. Pursue Gartner's "buy-smart" vendor contract cost optimization strategy.
2. Reinvest savings into new talent and security awareness training.

FAIR22 CONFERENCE

Key Takeaways

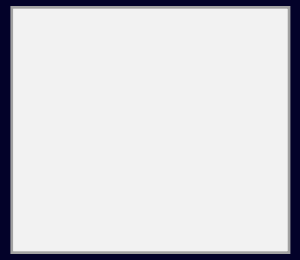
- Cyber risk now requires an enterprise-wide response
- Partner with ERM to develop a unified strategy for integrating CRM into the enterprise risk process
- Adopt an enterprise analytical model that enables ERM to more easily connect the dots across the enterprise, communicate the risk profile, and manage risk effectively.
- Friends in high places: Leverage that relationship to better position your perceived value

For information, please contact your Gartner representative

Primary 1:
Coquelicot

Primary 2:
Fun Blue

Secondary 1:
Gray95



Secondary 2:
Trolley Grey

FAIR22
CONFERENCE