RSAConference2018
San Francisco | April 16 – 20 | Moscone Center

SESSION ID: CXO-R14

INSIDE CYBER-BALANCE SHEETS: A RARE WINDOW ON DIGITAL RISK IN THE BOARDROOM

Yvette Connor

Chief Risk Officer
Focal Point Data Risk
@connoryk

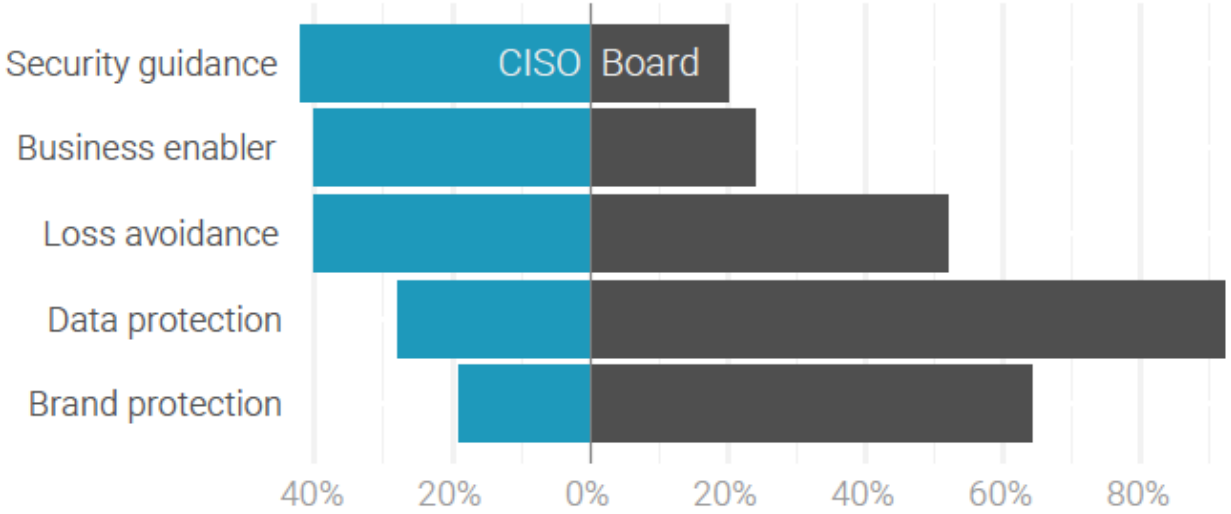
Wade Baker, Ph.D.

Founder, Cyentia Institute
Professor, Virginia Tech
@wadebaker

2017 CYBER BALANCE SHEET

What did we learn?

What is the primary value of cybersecurity to the business?



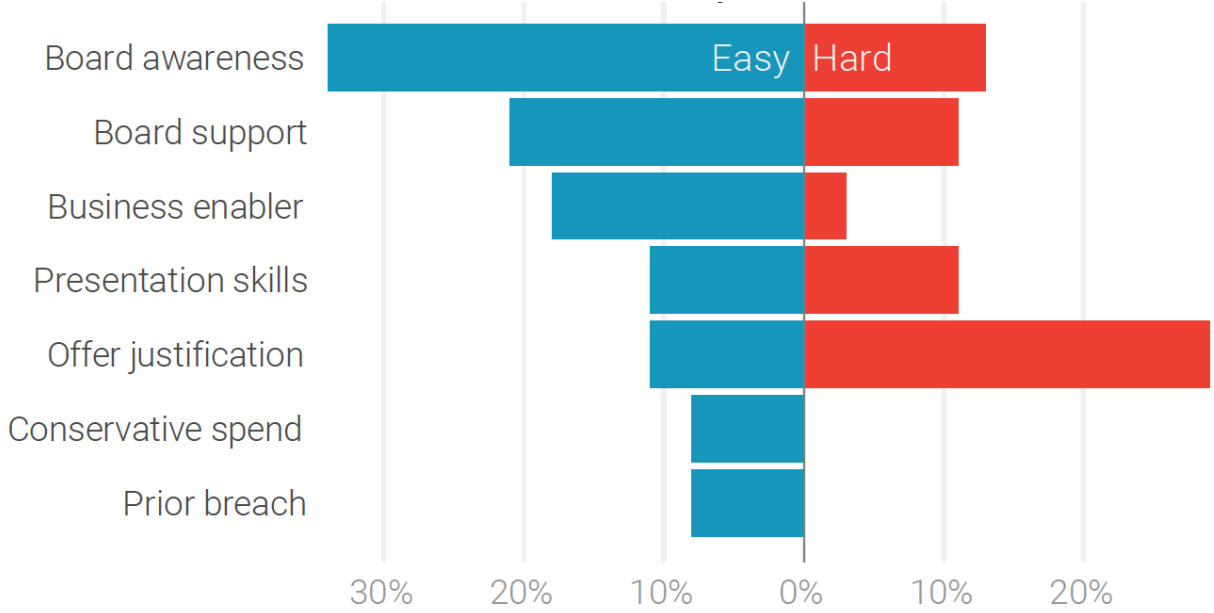
CISO PERSPECTIVE

"If I asked the Board, what my most important job is, they would say, 'Don't get breached.' But they get most upset when I don't respond promptly to sales inquiries."

BOARD PERSPECTIVE

"Trust is the #1 value security offers to the business. Trust that we can continue to do business without major breaches or disruptions."

What factors make it easier/harder to convey value?



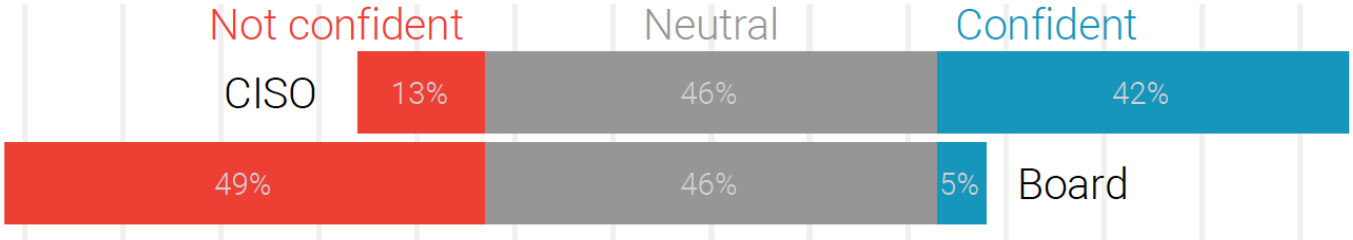
CISO PERSPECTIVE

"The main challenge is I could do everything right, and we could still have a loss. I could do everything wrong and nothing may happen."

BOARD PERSPECTIVE

"The value is hard to define and measure, which makes the Board skeptical. Security is such a broad topic that engaging all relevant parties to properly understand fiduciary liability is hard."

Are you confident with the security program's effectiveness?



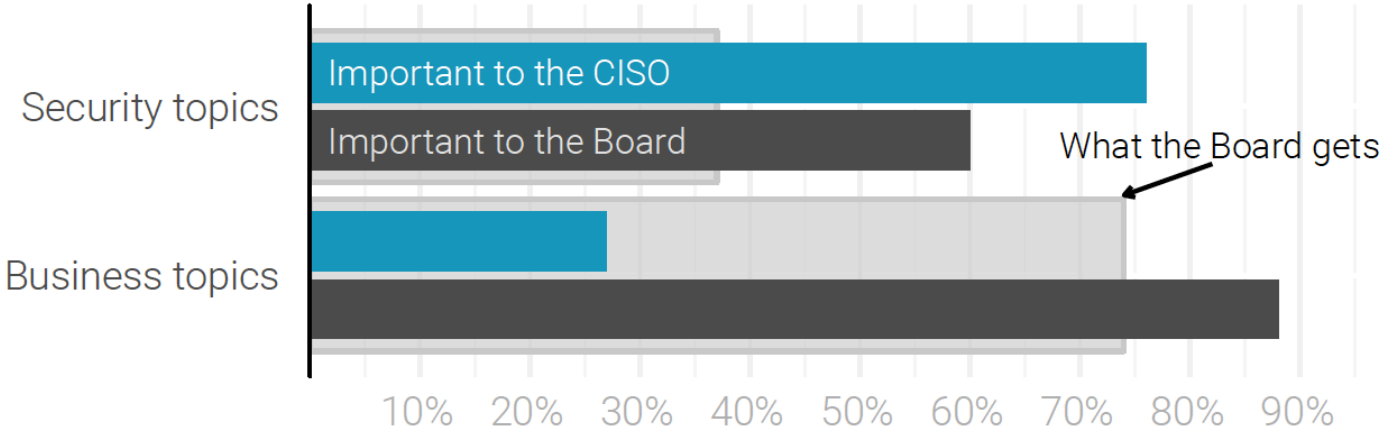
CISO PERSPECTIVE

"Several items are red at the moment. Not necessarily because they are high priority, but because there is a real risk. Green would make the Board ignore it."

BOARD PERSPECTIVE

"Directors come away with the overwhelming impression that no matter how much money they spend on security, they're still going to get breached."

What metrics are reported to the Board?



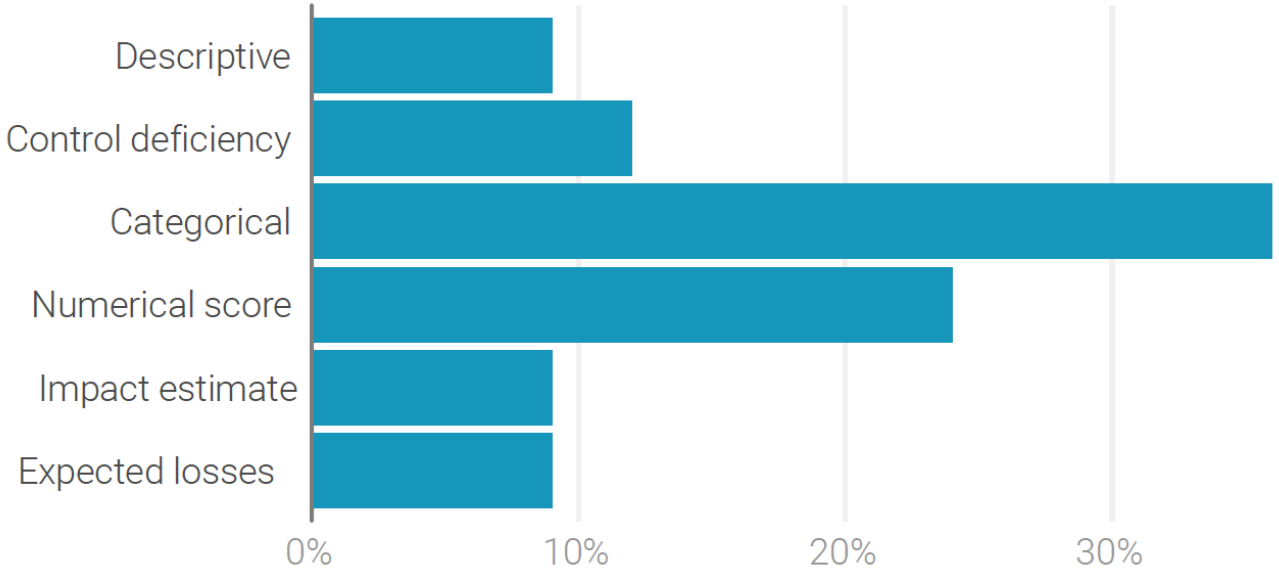
CISO PERSPECTIVE

"We had a weekly metrics report that was mostly useless when I came. I stopped it, but don't know what to replace it with. I don't think the industry knows what a successful security program looks like to measure against it."

BOARD PERSPECTIVE

"Stop talking about security. Talk about the outcomes of security. Does this help the business? Does it make my life better? What do we get that we didn't before? What do we eliminate that we had before?"

How is cyber risk measured in your organization?



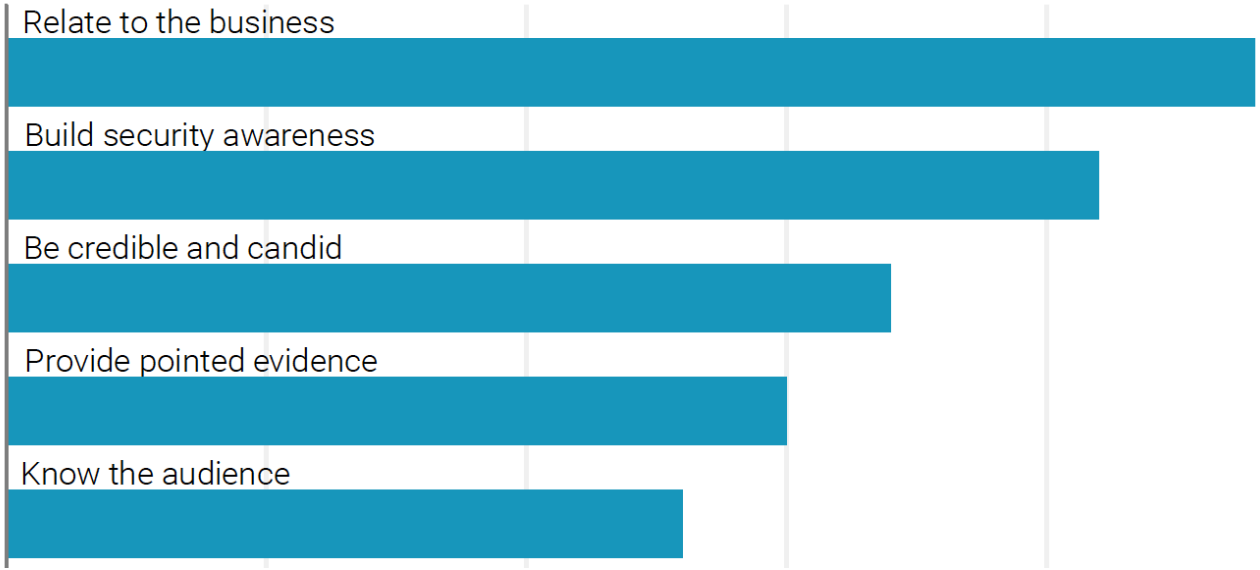
CISO PERSPECTIVE

"When there's a fire, I could calculate exactly how much water is needed to quench the flames, but it's usually better to just dump a bunch of water on it and move on to the next hot spot."

BOARD PERSPECTIVE

"The concept of measuring risk is important. Otherwise, it's just a list of things you've done and will do rather than a health metric."

Tips for communicating with the Board



*All 10 tips are in the Cyber Balance Sheet Report

BOARD PERSPECTIVE

"Security has a seat at the table but has nothing to say. We're listening, but security mumbles."

BOARD PERSPECTIVE

"Develop KPIs for the Board based on business initiatives rather than security products and processes."

Where are we Now?

Cyber Professionals	Boards and Executives	The Problems
Bottom-up, technology-led approach	Cyber risks not aligned with other enterprise risks	Wasteful investments
Balancing strategic and defensive	Struggling to meet oversight responsibilities	Unexpected risk
Responding to new threats	Motivated by operational and reputational risk concerns	Costly outcomes
Workforce skillset shortage	Complying with regulatory frameworks	Murky decisions (cyber insurance?)
		Regulatory actions

A CISO's Value Statement

I'm a CISO focused on
securing our client's Magic moments
by creating ***secure environments***
that ***enable*** *and* ***accelerate*** *the business*
and contribute to the
top and bottom line

Dinis Cruz, CISO Photobox, April 2017

Acknowledging Current Challenges

How to make rational risk-based decision
How to create high performance teams
How to scale security knowledge
How to drive and enable change
How to map data as graphs

Insights from the Boardroom

Boards tend to have **SIX** key questions:

How much cyber insurance should I buy?

Which of our cyber risk management options are likely to be most cost-effective?

How much risk is associated with…?

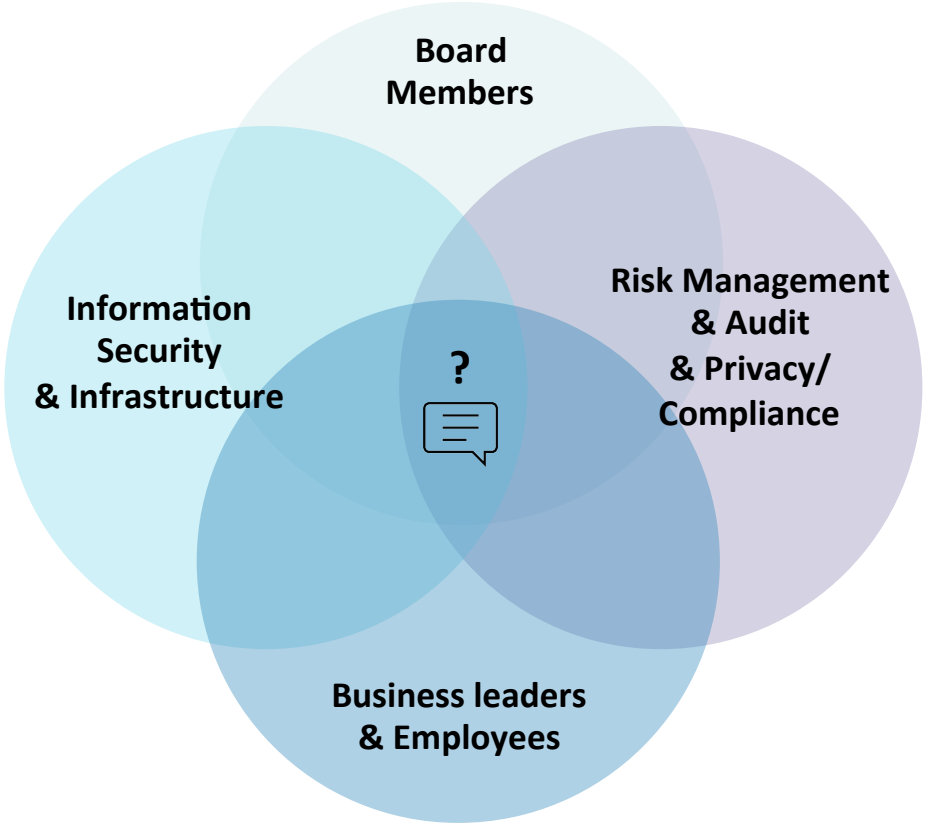
What benefit are we getting for our current cyber risk management expenditures?

How much cyber risk do we think we have and what is it from?

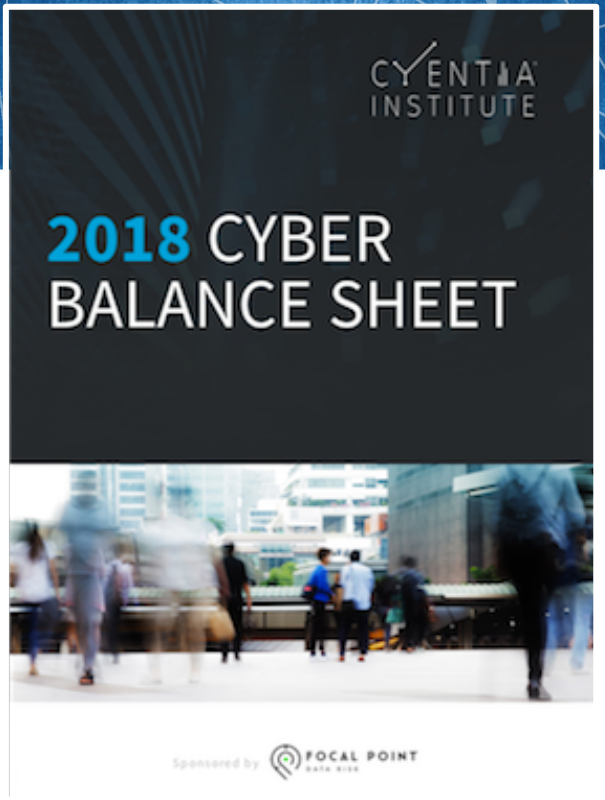
How much less (or more) risk will we have if…?

The questions are not complicated but, are difficult to answer in **simple**, **consistent**, and **measurable** terms.

What is Needed?



A **shared approach** for discussing the business aspects of cyber risk that meets the needs of all key stakeholders



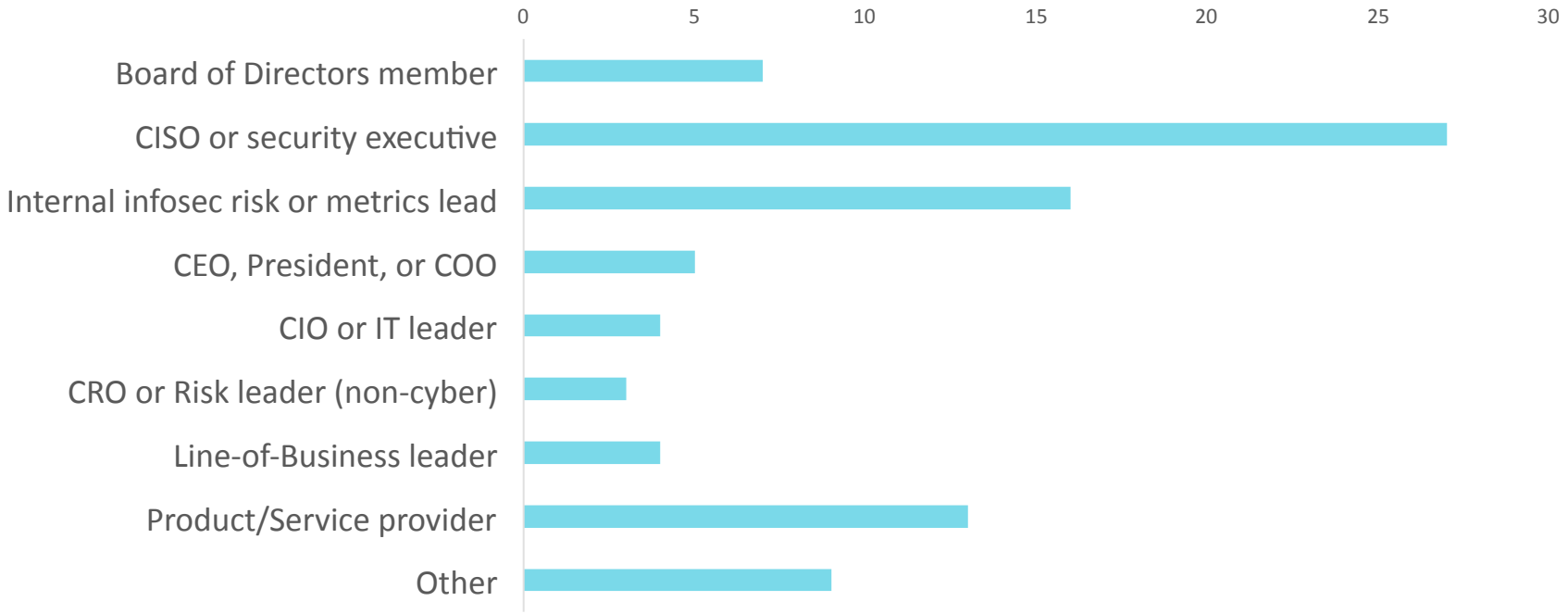
2018 CYBER BALANCE SHEET

What are we learning?

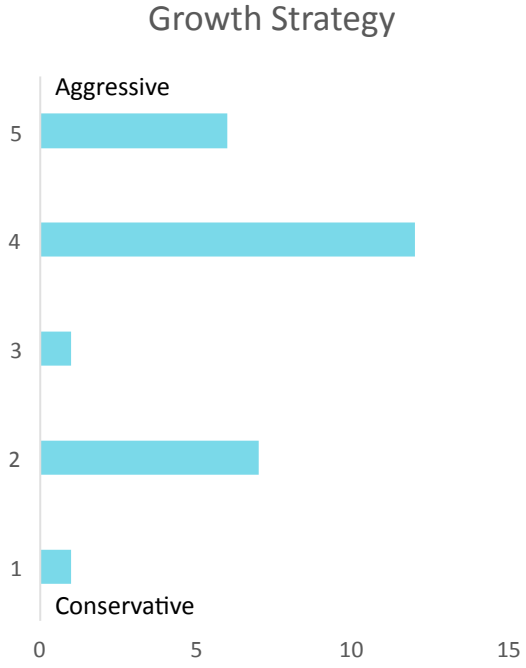
Research Questions for 2018

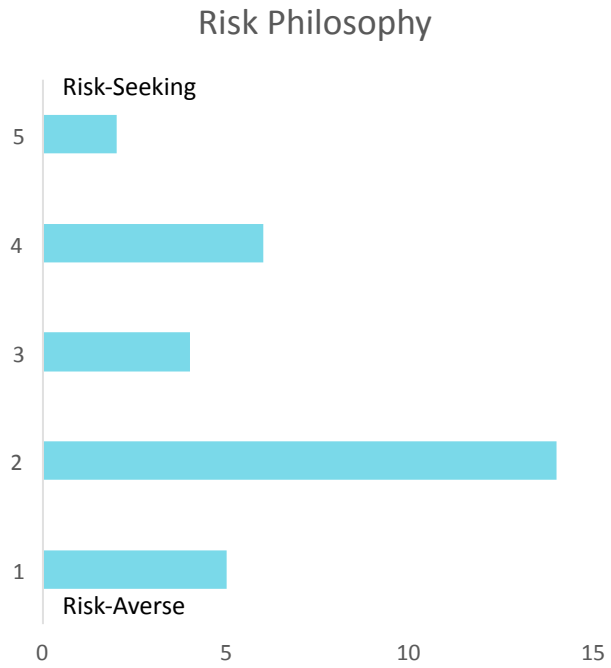
1. What is reported to the board?
2. How is it reported (e.g., format, context)?
3. Why is it reported?
4. How is it viewed by directors and other non-security execs?
5. How does all of the above differ among different types of orgs?

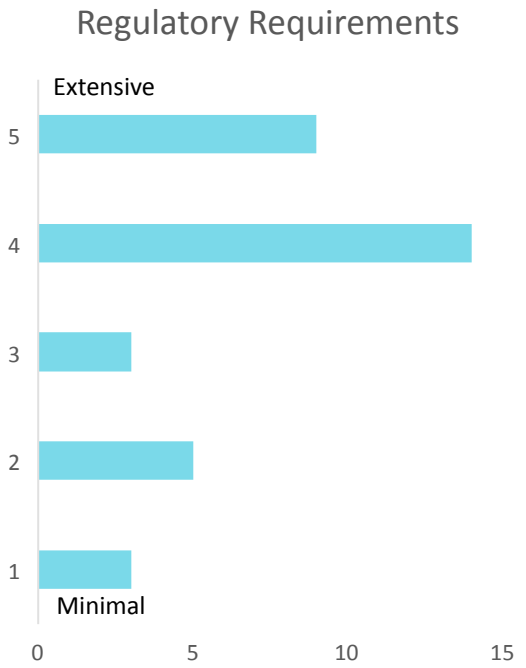
Participant role/title



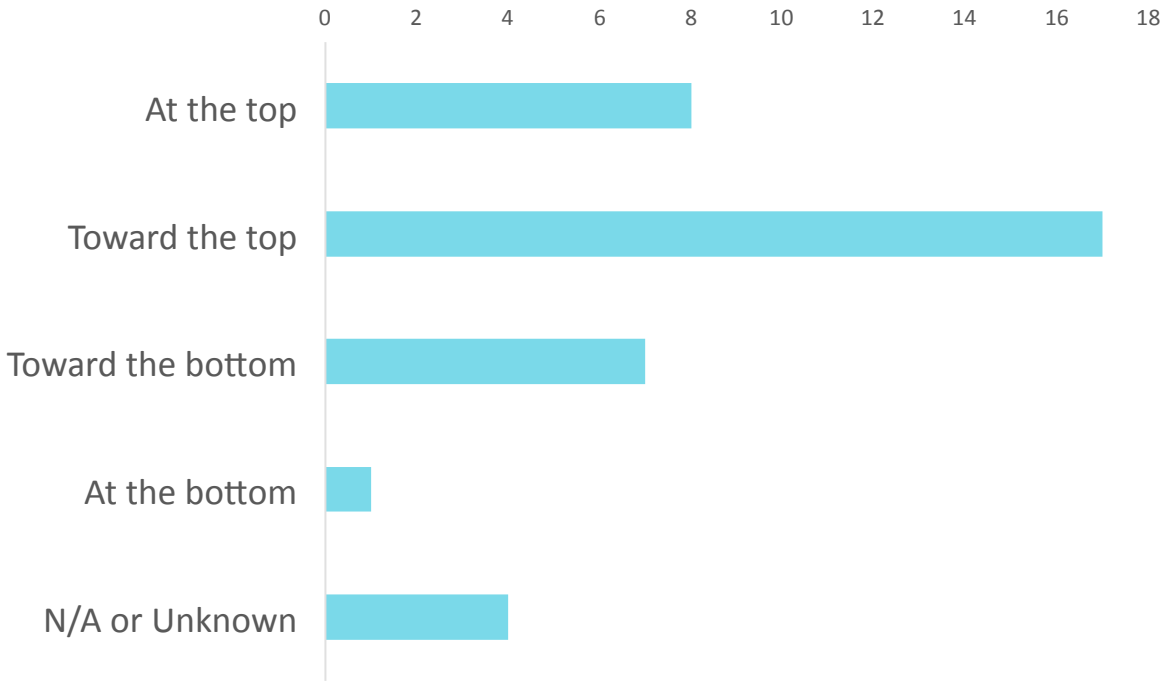
Organizational drivers







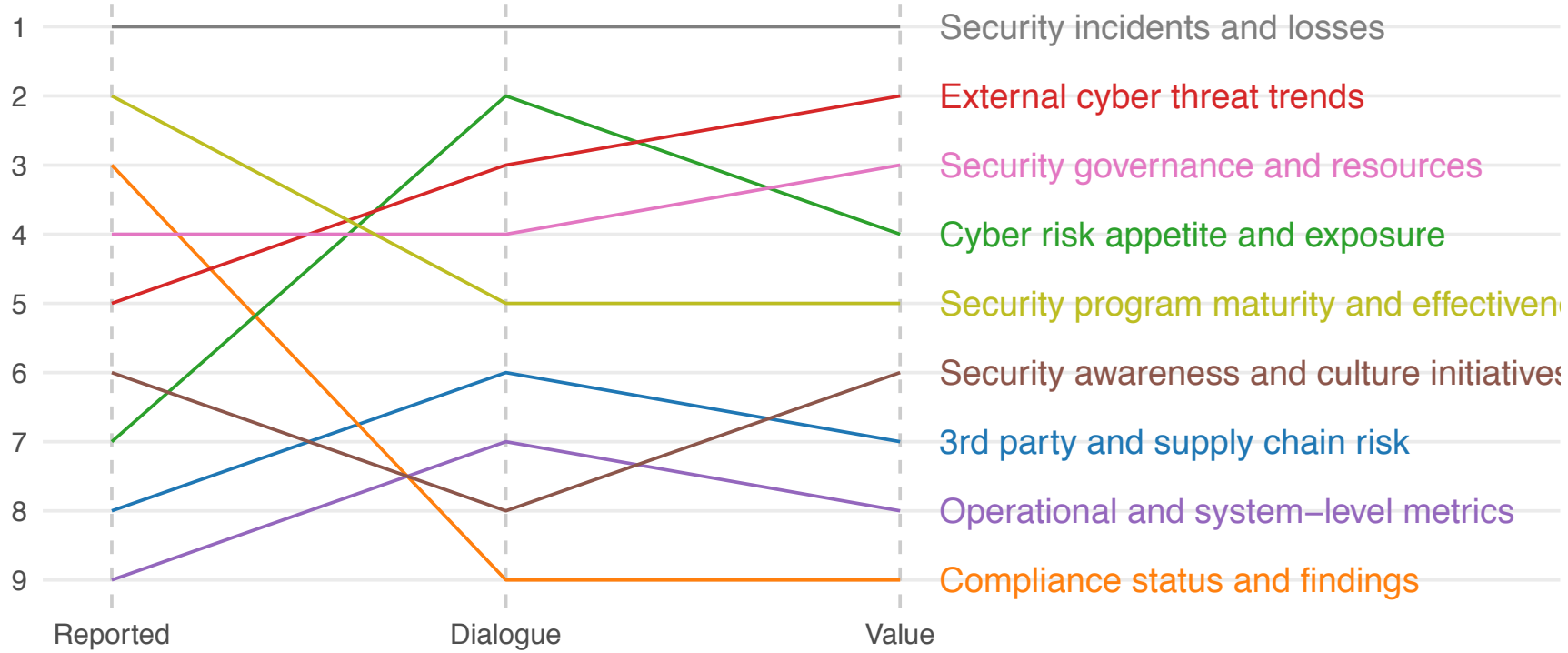
Compared to other sources of risk, where does cyber risk rank in terms of overall exposure?



"Cyber risk is one of the top 3 risks for the company. It is intrinsic to all services and products and is absolutely critical to the reputation of the company."

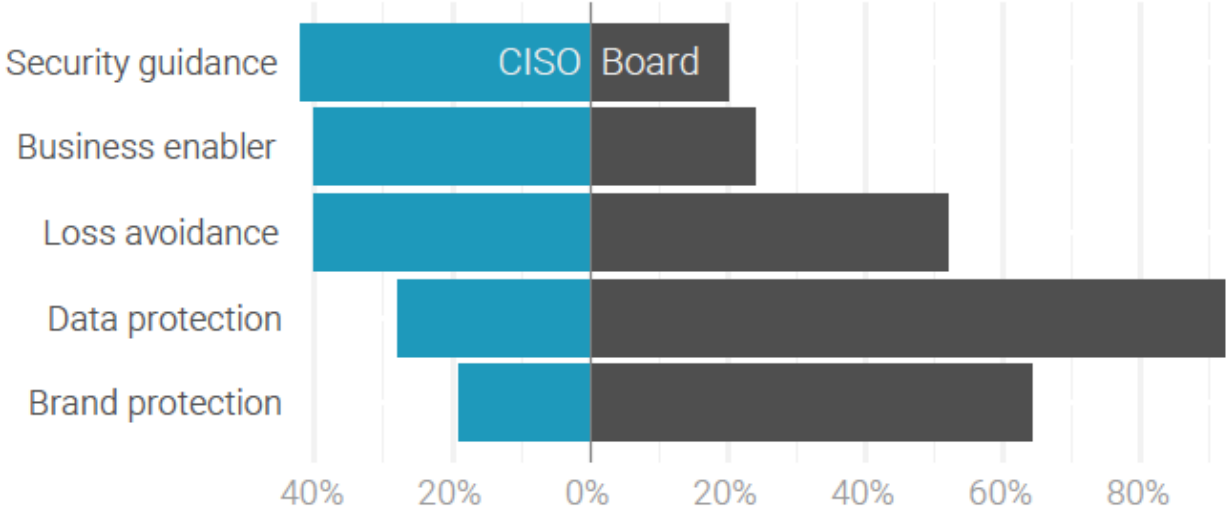
"We are an advanced stage mining exploration company… Cyber risk is not existential for us, unlike other companies."

Metrics reporting and perceptions



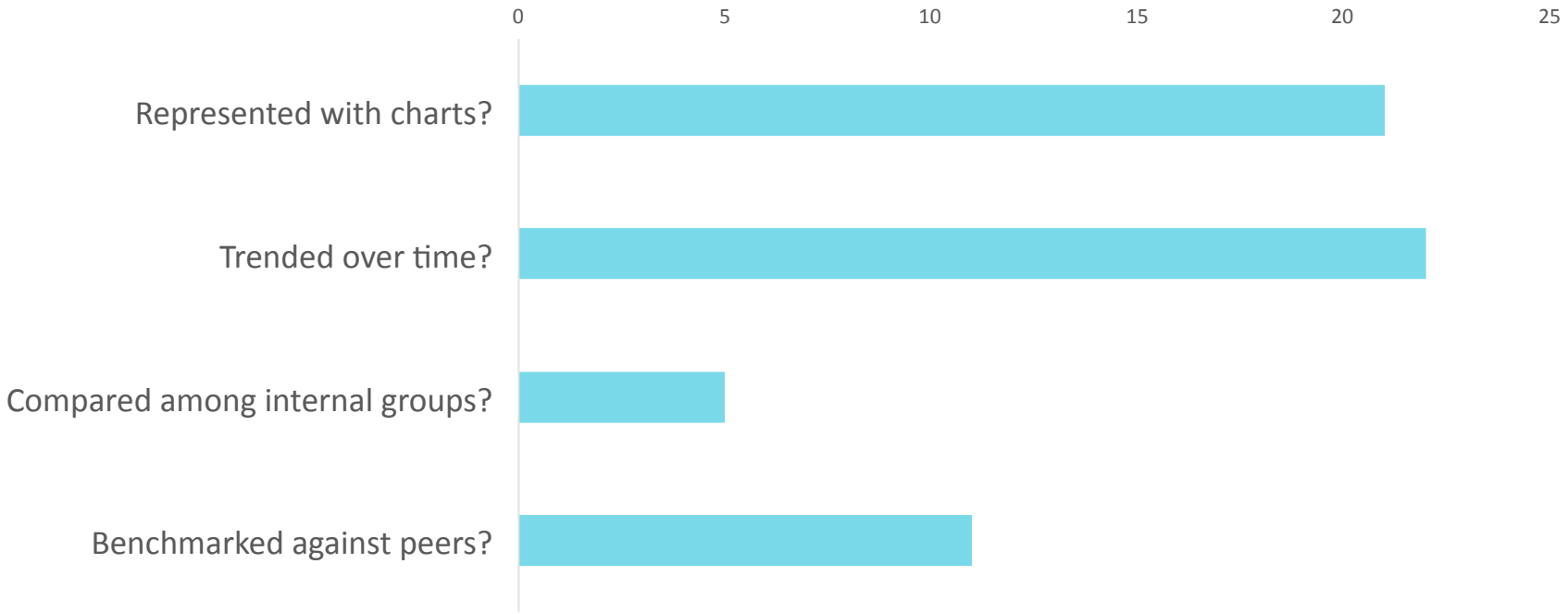
The Value of Cybersecurity

What is the primary value of cybersecurity to the business?



- Incidents and losses
- External threat trends

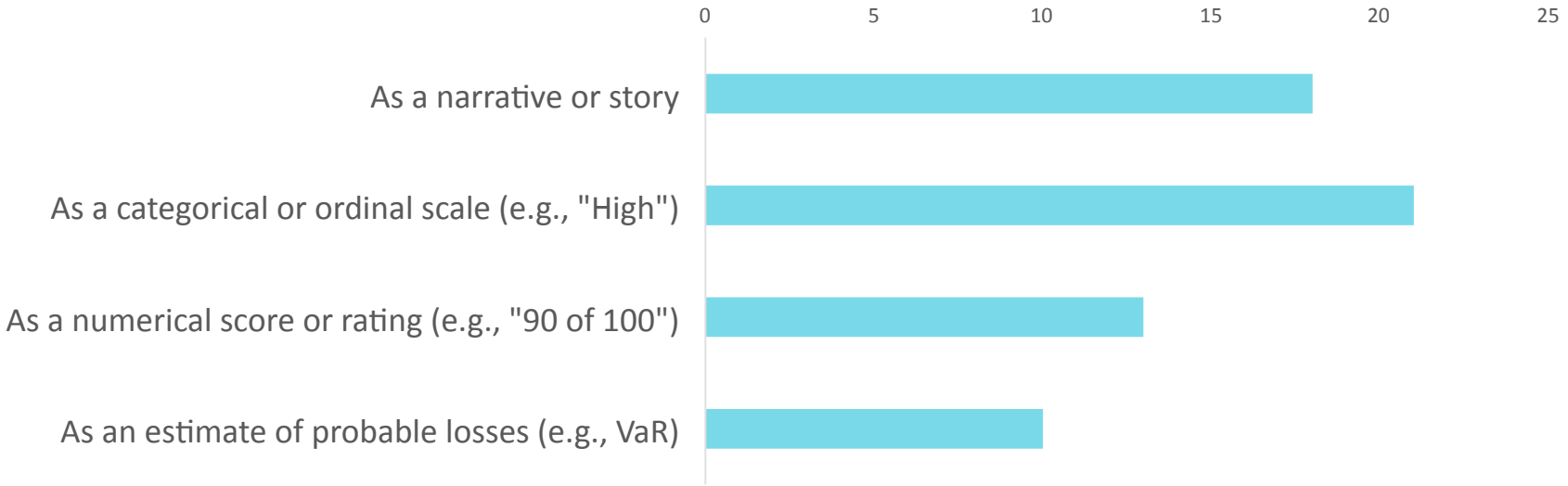
Are metrics reported to the Board…



Top challenges for clients?

"Making the information specific to client industry to be meaningful; Benchmarking; Providing predictive analysis and trending; Providing recommendations that have proven ability to reduce risk as measured through improved KPI at project level and KRI at organizational / operational level."

How is cyber risk expressed?



What is your organization's risk appetite?

"Probability of direct losses exceeding $25m and/or greater than 3% drop in sales due to reputational damage is less than 20% in next 12 months."

Have you established a cyber risk appetite?

Share your perspective

If you would like to participate in the current study, please email research@Cyentia.com

Thank you!

FOCAL POINT DATA RISK

CYENTIA INSTITUTE