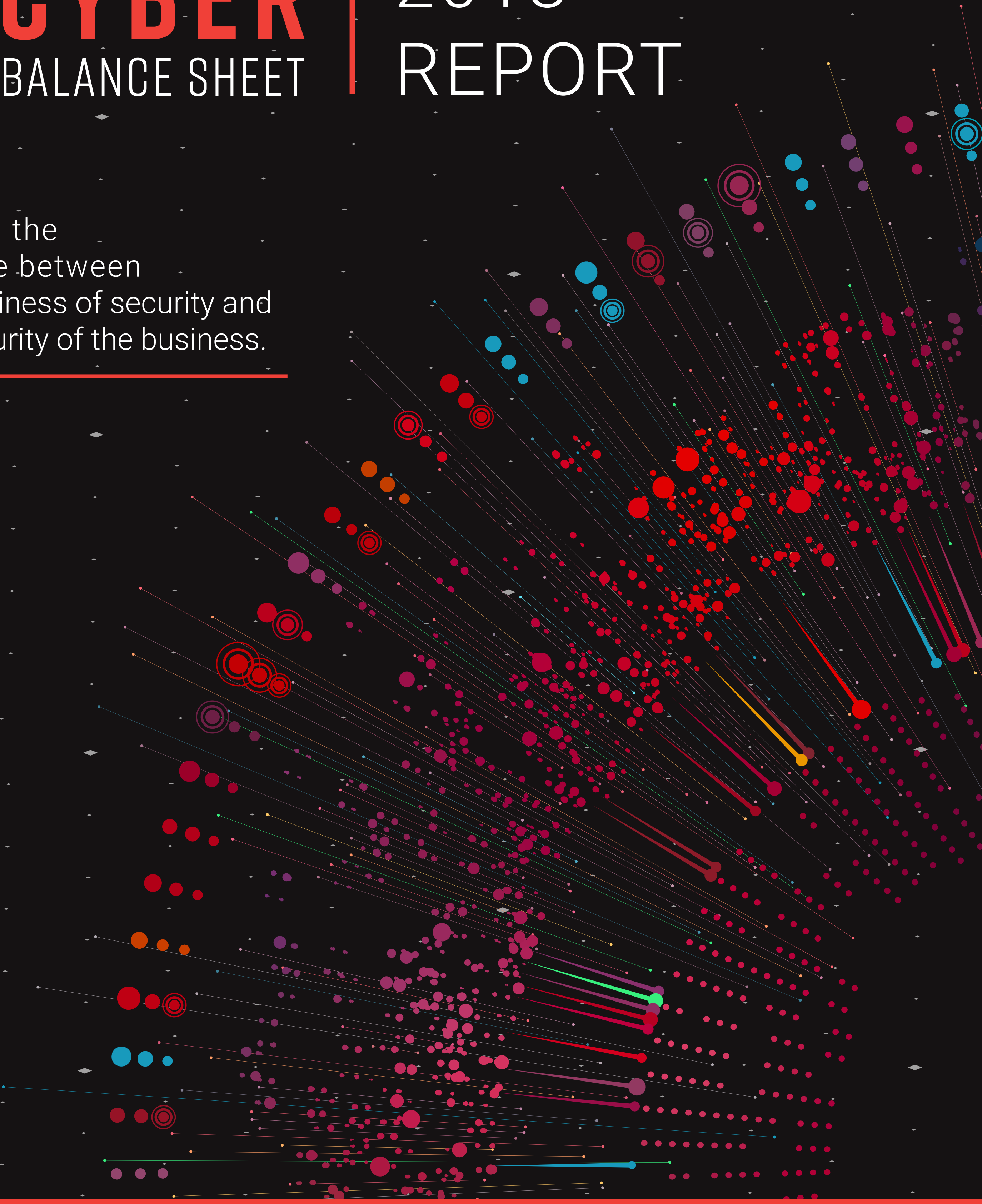
CYBER BALANCE SHEET | 2018 REPORT

Finding the
balance between
the business of security and
the security of the business.



sponsored by: FOCAL POINT DATA RISK

WELCOME BACK!

We're glad you've decided to join us for the second installment of an ongoing study by Focal Point Data Risk and the Cyentia Institute to improve consensus and communication around cyber risk. In last year's report, we sought to break down walls of misunderstanding between cybersecurity leaders and corporate directors. We continue chipping away at those walls this year, but expand the scope of our research to include a broader set of stakeholders and topics relevant to our increasingly important goal.

You can get a sense of those topics from the Table of Contents. If you're new to this report series, the "Looking Back and Moving Forward" section should get you up to speed quickly (but we do recommend adding the 2017 Cyber Balance Sheet Report to your reading list for later). Though each "Balance Point" is self-contained, we suggest reading them in order, as they build upon one another as the report progresses. We hope each point helps in achieving the difficult balance between the "business of security" and "security of the business."

ABOUT OUR SPONSOR

FOCAL POINT
DATA RISK

Focal Point Data Risk is a new type of risk management firm, one that delivers a unified approach to addressing data risk through a unique combination of service offerings. Focal Point has brought together industry-leading expertise in cyber security, identity governance and access management, data privacy and analytics, internal audit, and hands-on training services, giving companies everything they need to plan and develop effective risk and security programs. By integrating these services, we provide our clients with the flexible support they need to protect and leverage data across any part of their organization. Simply put, Focal Point is the next generation of risk management.

focal-point.com   @focalpointdr   in Focal Point Data Risk

ABOUT THE RESEARCH

CYENTIA®
INSTITUTE

Analysis for this report was provided by the Cyentia Institute. Cyentia seeks to advance cybersecurity knowledge and practice through data-driven research. We curate knowledge for the community, partner with vendors to create analytical reports like this one, and help enterprises gain insight from their data.

cyentia.com   @cyentiainst   in Cyentia Institute

TABLE OF CONTENTS

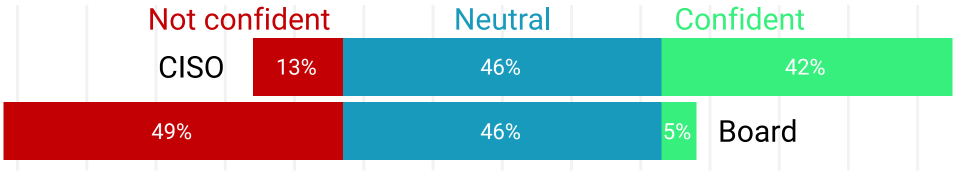
If you have comments or questions while reading, we encourage you to join the conversation using #CyberBalanceSheet and connecting with us on Twitter (@cyberblncesheet) or LinkedIn.

LOOKING BACK AND
MOVING FORWARD

Our stated objectives for the 2017 Cyber Balance Sheet Report were to gather perspectives, characterize key issues, identify possible solutions, and draw cybersecurity and business leaders together through greater shared understanding and purpose. Turns out those were appropriate goals because our findings showed divergence on even fundamental issues like the role and value of cybersecurity to the business, which inevitably erodes confidence at the top.

FIGURE 1: BOARDS LACK CONFIDENCE IN THE SECURITY PROGRAM

In the 2017 Report, few CISOs expressed doubts about the efficacy of their program, but board members appeared far more skeptical.



> **DIRECTORS GET THE OVERWHELMING IMPRESSION THAT NO MATTER HOW MUCH MONEY IS SPENT ON SECURITY, THEY'RE STILL GOING TO GET BREACHED.**

The key question is why this lack of confidence exists. Based on interviews with both groups, we learned that confidence and communication go hand in hand. In particular, misalignment and miscommunication of key performance and risk metrics lies at the root of doubts among board members.

FIGURE 2: BOARDS PREFER BUSINESS-LEVEL SECURITY METRICS

Our 2017 Report found that CISOs value operational security metrics, but boards want information tied to business-level outcomes.

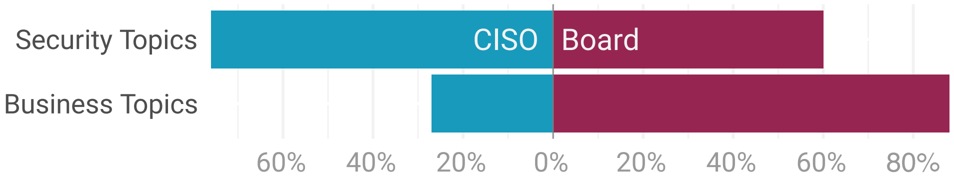
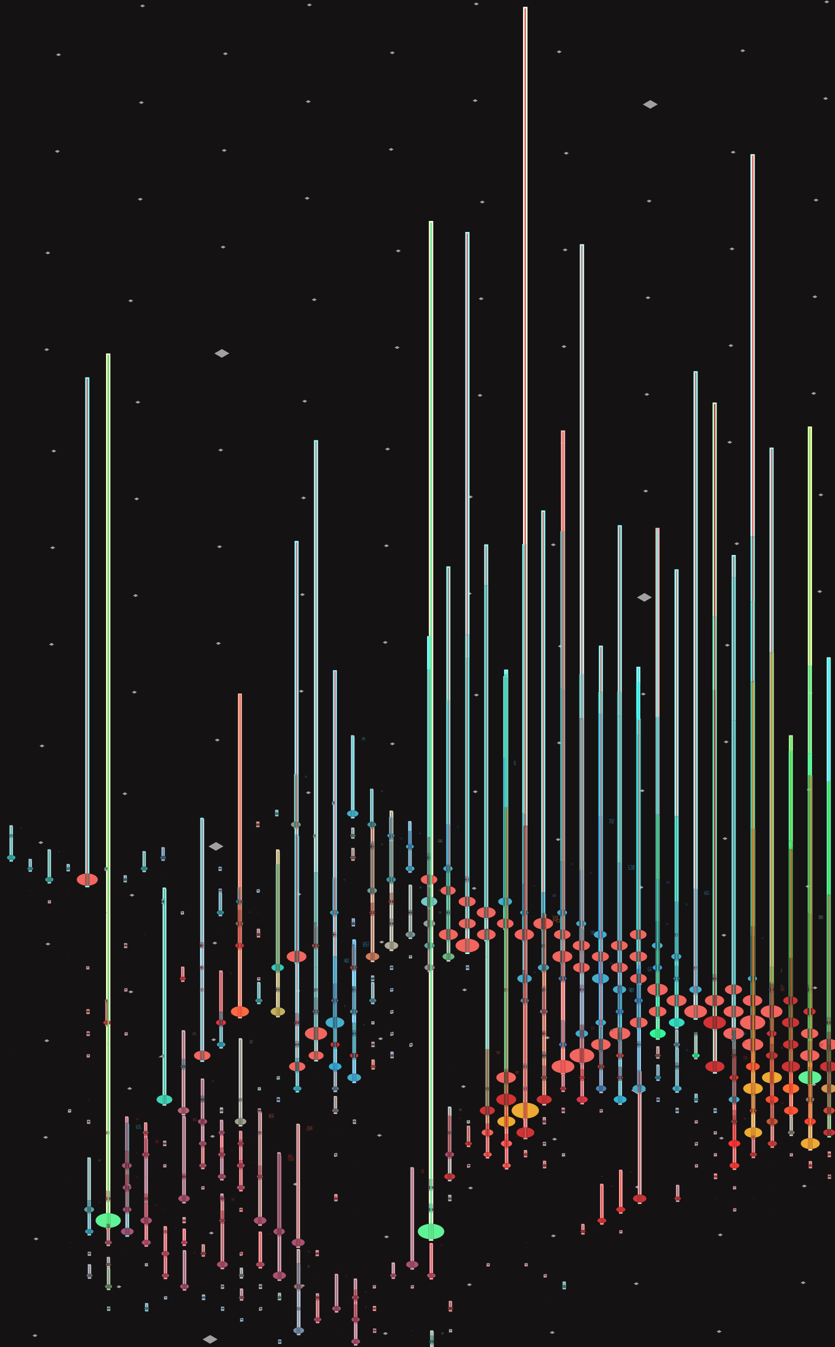


Figure 2 illustrates this dilemma well. When asked what information they find most valuable for understanding the cybersecurity posture of the company, boards crave far more business-relevant reporting than CISOs. While this disparity may not be shocking, clearly a better path forward is needed. The goal of this follow-up study is to find that path and help organizations get started down it.

2018 RESEARCH QUESTIONS

1. How is cyber risk perceived relative to other types of risk? What factors alter this perception?
2. What cyber risk information is reported to the board? What drives dialogue and value?
3. How is cyber reporting viewed by the board? What drives confidence and satisfaction?
4. How does cyber risk reporting – and reception – vary across roles and organizations?



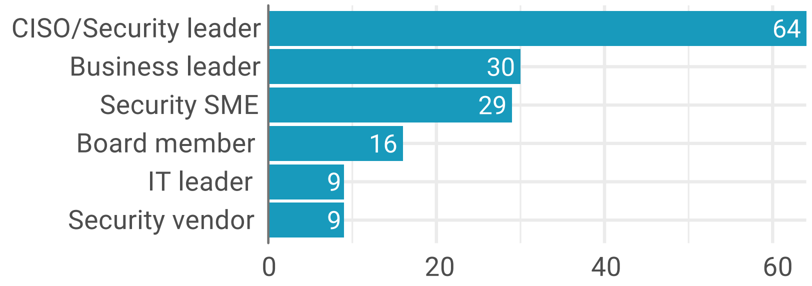
> **"STOP TALKING ABOUT SECURITY. TALK ABOUT THE OUTCOMES OF SECURITY. DOES THIS HELP THE BUSINESS? WHAT DO WE GET OR ELIMINATE FROM BEFORE?**

METHODOLOGY AND SAMPLE DEMOGRAPHICS

Based on these research goals and questions, we determined a survey offered the most suitable data collection method. The interview format used in the 2017 Report worked well for the open-ended, exploratory nature of that study, but digging deeper into the issues requires a more standardized dataset.

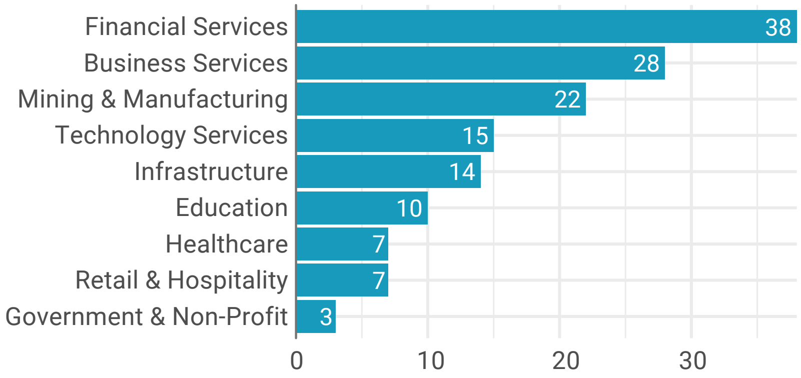
Obtaining a representative sample for cybersecurity surveys is notoriously difficult, especially when corporate directors and executives are sought. Our initial sampling frame was comprised of prior interviewees and contacts gained from the last report. We utilized a snowball sampling technique from there, asking for introductions to other qualified respondents. To further improve our reach, we collaborated with several other entities to distribute the call for participation to their members (see list in the Acknowledgements). Key demographics for the resulting sample are provided below.

FIGURE 3: SUMMARY OF RESPONDENT ROLES



Of the 157 validated respondents to our survey, 38% were CISOs (by title or function). Another 18% held other security roles, typically related to risk management and metrics. A large contingent from the C-suite (14 CIOs, 13 CEOs, 7 CFOs, 3 CROs, 3 CAEs) and a smattering of other business leaders participated. Several security product and service vendors lent their clients' perspectives to the effort too.

FIGURE 4: SUMMARY OF INDUSTRIES REPRESENTED



Industry categories are found in Figure 4. Slicing the data nine different ways quickly gets cumbersome, so we often simplify this list down to public for-profit (44%), private for-profit (37%), and non-profit (15%).

Our sample skews regionally, with about two-thirds of organizations based in the U.S. Much of the remainder (20%) hail from Europe.

FIGURE 5: SUMMARY OF ORGANIZATION SIZE

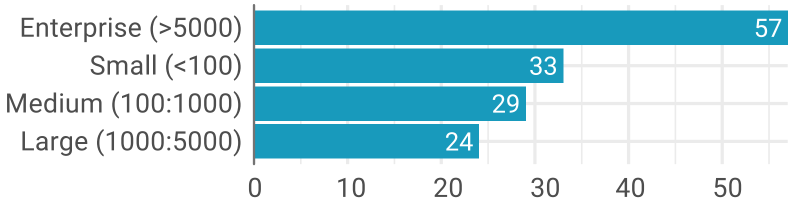


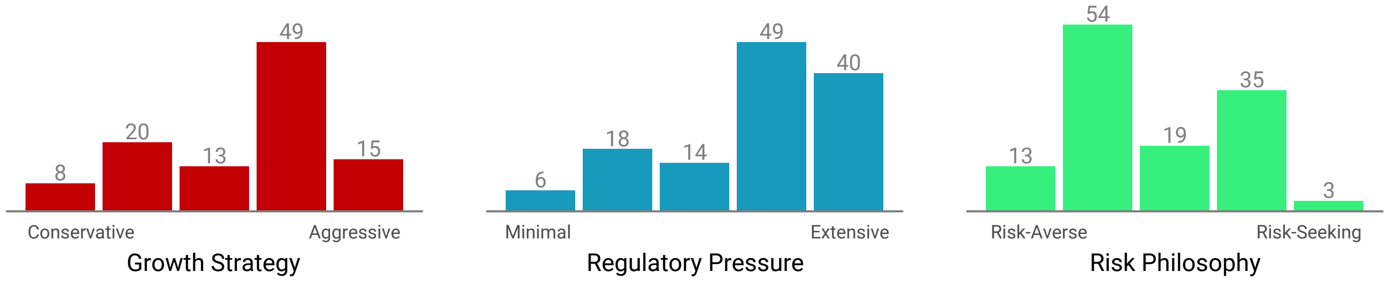
Figure 5 offers a view of organizational size based on the number of employees. From this, it's obvious our sample leans toward larger enterprises, yet gives SMBs a voice in the results too. Half of participating firms report more than $250 million in annual revenue. About one in four fall below $10 million.

BALANCE POINT 1:
EXPLORING ORGANIZATIONAL RISK DRIVERS

Demographics offer useful information on a sample, but paint only part of the picture when trying to understand what drives organizational perceptions of and approaches to cyber risk. It is commonly assumed shared demographics equate to shared cyber risk profiles — and some evidence to support this does indeed exist[1] — but how far can we take that? Should all financial services firms measure, manage, and communicate cyber risk in the same manner? Surely other factors drive such decisions.

FIGURE 6: RATINGS FOR ORGANIZATIONAL RISK DRIVERS

Firms exhibit different perceptions of and approaches to growth, regulation, and risk.



To explore this, we asked respondents where their firms stand on three common business drivers:

1. Revenue growth strategy (conservative to aggressive)
2. External regulatory pressures (minimal to extensive)
3. Risk management philosophy (averse to seeking)

It's often said that regulation and/or risk-aversion stifles growth, but Figure 6 makes it clear that many organizations would prefer to have their cake and eat it too. Overall, these results reveal the balancing act that successful business leaders must master: maintain strong growth in the face of mounting regulatory pressures without taking on too much risk.

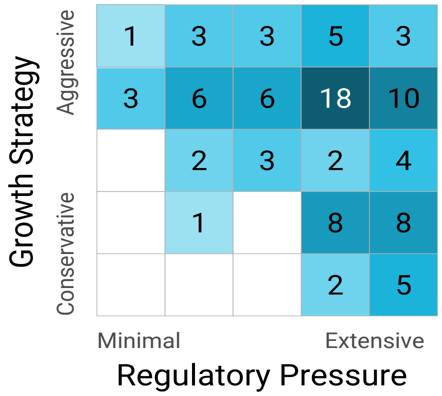
But Figure 6 doesn't tell the whole story. Its generalized view loses fidelity that may yield insight to our research questions. The fact is that most organizations are not "all of this and none of that." Each is unique, and these drivers combine in subtle ways to influence goals, strategy, and execution. Given that, let's see what we can learn about the relationship between these drivers.

> “ WE AGGRESSIVELY SEEK TO GROW REVENUE, YET ARE ALWAYS ENSURING THE RISKS AND COSTS OF COMPLIANCE DON'T OUTWEIGH THE BENEFIT.

[1] *For example, Verizon's Data Breach Investigations Reports regularly highlight threats common to particular industries.*

Figure 7 compares regulatory pressure and growth strategy and shows the number of firms at the intersection of each level (i.e., 10 firms rated a 5 for regulation and a 4 for growth). While most organizations rate high on both axes, a fairly wide range of regulation-growth combinations exist. That is not to say regulations have no relationship to growth; they just don't appear to impact the goal or strategy to grow the business.

> **OUR RISK HERE IS LARGELY DEPENDENT ON THE REGULATORS. LAWS CHANGE FREQUENTLY AND COULD ADVERSELY IMPACT THE COMPANY OVERNIGHT.**

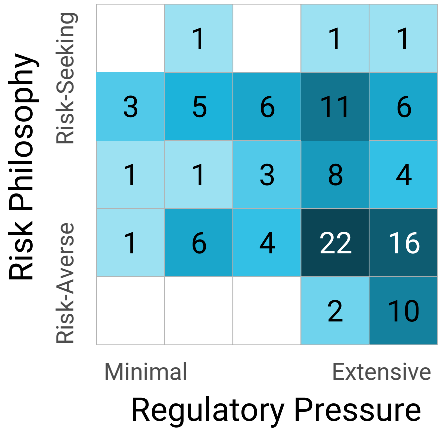


1	3	3	5	3
3	6	6	18	10
	2	3	2	4
	1		8	8
			2	5

FIGURE 7:
REGULATION VS. GROWTH

Figure 8 suggests a firm's risk philosophy is inversely correlated with regulatory pressures. Highly-regulated firms do indeed tend to be risk-averse, but that's not a hard and fast rule. Notably, several healthcare providers occupy "high regs, high risk" quadrant in the upper right. Though not shown in the figure, the majority of respondents said external regulations strongly influence their strategy for managing cyber risk.

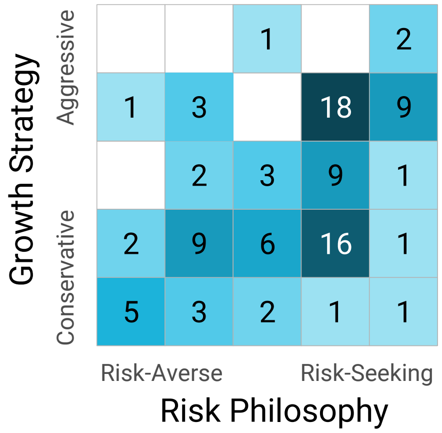
> **WHILE WE MAKE NECESSARY RISK TRADEOFFS TO DELIVER VALUE AND MAINTAIN LONG-TERM SUSTAINABILITY, WE DO SO IN A SAFE AND SOUND MANNER.**



	1		1	1
3	5	6	11	6
1	1	3	8	4
1	6	4	22	16
			2	10

FIGURE 8:
REGULATION VS. RISK

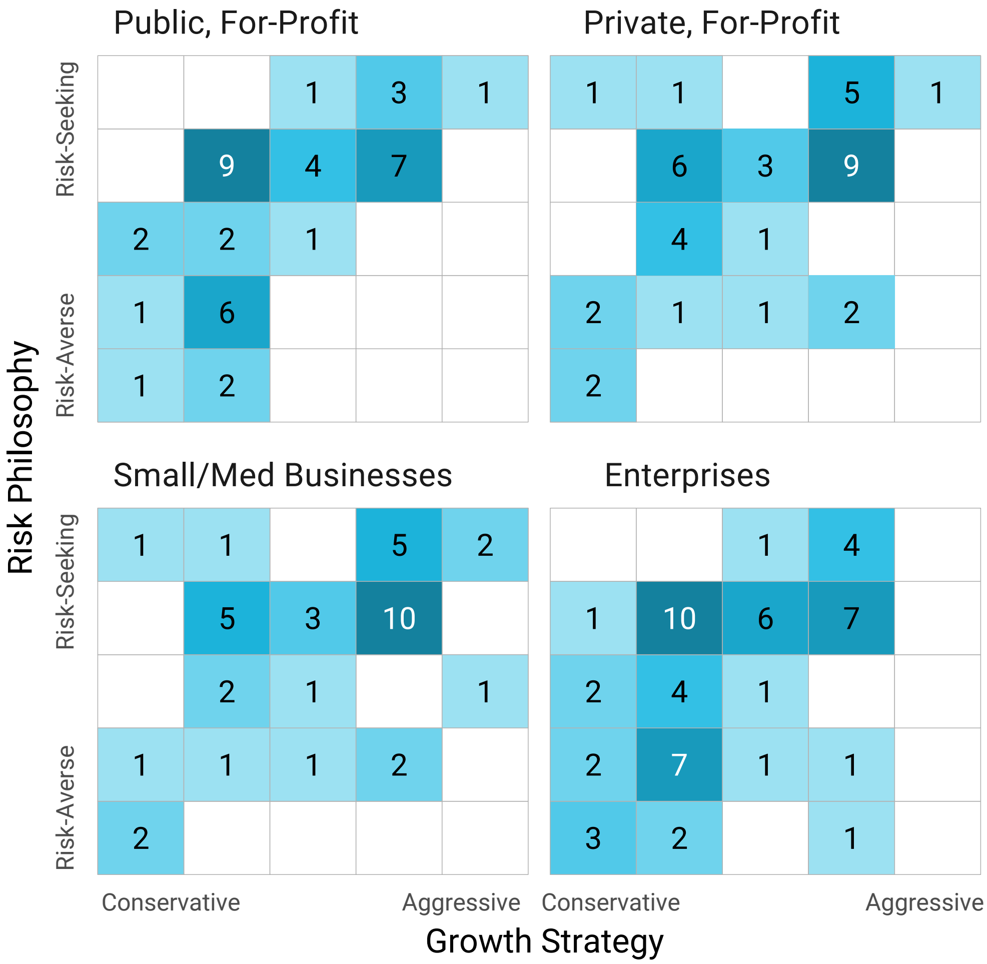
Figure 9 shows a comparison of risk philosophy and growth strategy. The highest count of firms falls in the upper right quadrant, but a surprising number occupy the lower end of both axes as well. In theory, these drivers should be aligned to enable the organization to pursue its goals. But the sizeable contingent in the risk-seeking, conservative growth range indicates that is not always the case.



		1		2
1	3		18	9
	2	3	9	1
2	9	6	16	1
5	3	2	1	1

FIGURE 9:
RISK VS. GROWTH

FIGURE 10: SAMPLE DEMOGRAPHIC COMPARISON FOR RISK VS GROWTH



Public, For-Profit

		1	3	1
	9	4	7	
2	2	1		
1	6			
1	2			

Private, For-Profit

1	1		5	1
	6	3	9	
	4	1		
2	1	1	2	
2				

Small/Med Businesses

1	1		5	2
	5	3	10	
	2	1		1
1	1	1	2	
2				

Enterprises

		1	4	
1	10	6	7	
2	4	1		
2	7	1	1	
3	2		1	

It's tempting to explain patterns among these drivers based on shared demographics, as we did with healthcare for *Regulation vs. Risk* above). But Figure 10 cautions against applying this logic too widely. The top two matrices compare public vs. private companies, and the bottom two compare SMBs with larger enterprises. In each case, we see both convergence and divergence. The takeaway here is that even similar types and sizes of firms can vary widely in their goals and tolerances. This undoubtedly affects how they view and approach cyber-specific risk. Because of this, we use these classifications as lenses through which to view findings and organizational comparisons in the following Balance Points.

WHERE TO FOCUS

These findings validate that risk drivers vary by firm, regardless of demographic profile. This is key to understanding how cyber risk influences and supports the business. It's also a helpful guardrail against simplistic "because you're this, you must be like that" analytical approaches.

BALANCE POINT 2:

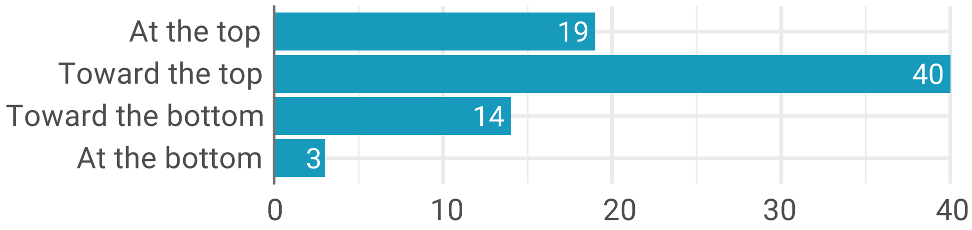
PUTTING CYBER RISK IN PERSPECTIVE

Organizations have a lot to consider when it comes to managing risks to the business. By most reports, cybersecurity has been climbing that list of considerations for years. But where cyber risk stands today relative to other sources of risk is a matter of perspective, as the quotes in this section indicate.

To add structure to those quotes, we asked respondents where cyber risk ranked in their organization's stack of risks. Figure 11 shows their position on that comparison.

FIGURE 11: RANKING OF CYBER RISK TO OTHER ENTERPRISE RISKS

The majority of respondents rank cyber risk at or toward the top of risks facing their organizations.



The largest group of respondents ranks cyber risk "toward the top" but not "at the top." Very few put it at the bottom of the stack. Overall, the upper vs. lower split closely approximates the 80-20 rule. We don't have time-series data, but we can't help but imagine an increasingly top-heavy rebalancing over the last decade or so. Will cyber risk ever stand firmly at the top? Well, that probably depends on who you ask.

HOW DOES CYBER RISK RANK?

> " WE ARE AN ADVANCED STAGE MINING EXPLORATION COMPANY. CYBER RISK IS NOT EXISTENTIAL FOR US, UNLIKE MANY OTHER COMPANIES.

> " 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 OUR REPUTATION.

FIGURE 12: RANKING OF CYBER RISK TO OTHER RISKS BY ROLE

Respondents with security roles are far more likely to rank cyber risk at or toward the top of all types of risk to their firms.

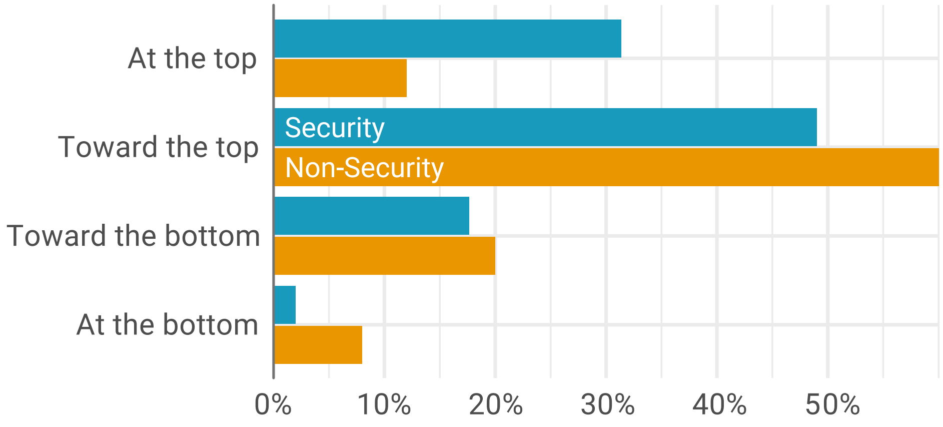


Figure 12 proffers an explanation. About one-in-three respondents in security roles place cyber risk at the top — far more likely than their business counterparts. There's undoubtedly one or more of the many cognitive biases at work here, which warp the way we all see the world (especially our neck of the woods). Understanding how to recognize and compensate for this may help avoid some of the imbalances observed in our last report.

> **"CYBER RISK HAS BEEN INCREASING DUE TO THE NUMBER OF CYBER SECURITY EVENTS IN THE NEWS, RAISING AWARENESS OF THE ISSUE."**

Aside from role, we wanted to explore what other factors might contribute to an organization's perception of cyber risk relative to other risks. Since there are so few "at the bottom," we'll start there. It would be convenient if we could simply put these three black sheep in one shared pen, but they're not having it. Here's the breakdown:

- A large financial services company in Australia
- A 500-employee private for-profit firm in the US
- A small non-profit educational institution in the US

There's not much to latch onto among those three, which we find quite interesting in light of the previous section. The data won't allow correlations for these qualitative factors, but those that appear most prominent among organizations ranking cyber risk "at the top" include:

- Public for-profit companies
- Firms with aggressive growth strategies
- Larger enterprises (>5K employees)

The financial services industry was also strongly represented among firms claiming top-level regard for cyber risk, but it led those in the lower half of Figure 11 as well. Thus, we left those to cancel each other out and did not include it above.

One last point bears mention before closing out this section. We expected factors like risk philosophy and regulatory pressures to shape responses on this topic, but that does not seem to be the case — or at least not strongly. We believe this makes it even more imperative that cybersecurity and business leaders work together to assess and manage risks — of all types — to the business.

WHERE TO FOCUS

Cybersecurity teams would do well to remember that directors and executives deal with a wide range of risks, some of which may be more critical to the vitality of the business. Focus on providing sound estimates and counsel on cyber risk so they can make informed comparisons and decisions.

NOTES FROM THE FIELD

> “WE’RE NOT OVERLY CONCERNED ABOUT RISK TO PII; RATHER THE OPERATIONAL RISK IS WHAT KEEPS US UP AT NIGHT.

> “CYBER THREATS PROVIDE A CHANNEL THROUGH WHICH TO DISPROPORTIONATELY IMPACT THE BUSINESS, HENCE, ITS PROMINENCE.

BALANCE POINT 3:

ESTABLISHING CYBER RISK APPETITE AND EXPOSURE

We've learned that cyber risk ranks relatively high on the "risk radar" for the majority of organizations. But how does that comparison translate into a firm's cyber risk appetite?

If you're unfamiliar with the term, risk appetite is generally defined as the amount and type of risk an organization is willing to accept. Establishing and communicating a coherent risk appetite is essential to successfully balancing the risk drivers discussed in Balance Point 1. Without this, answering questions like "how much risk are we willing to accept for x amount of growth?" is nigh impossible.

We learned earlier that more organizations identify as "risk-averse" than "risk-seeking," but that doesn't equate to a formal statement of risk appetite. About 70 respondents gave some form of input when asked for their organization's overall risk appetite, and 25 of those also provided an answer specific to cyber risk appetite.

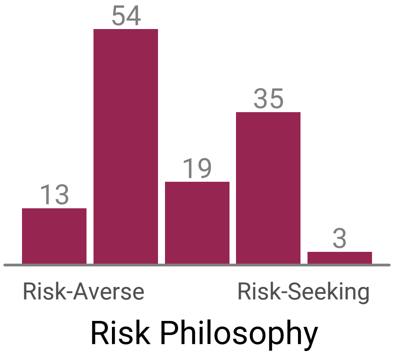
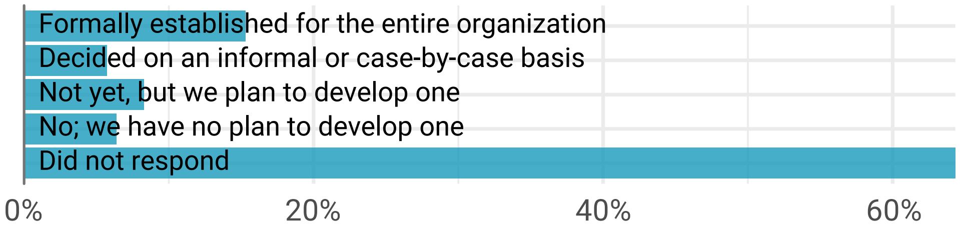


FIGURE 13: FIRMS LEAN TOWARD RISK-AVERSION

FIGURE 14: HOW IS CYBER RISK APPETITE DEFINED?

Many firms lack a defined cyber risk appetite, making it difficult to answer "Are we secure enough?"



Unfortunately, we cannot determine the exact reason(s) for that low response rate, but we can infer from Figure 14 that many organizations have not formally established a cyber risk appetite or aren't aware of its existence. Either way, this leaves a large majority of organizations in a grey zone of making things up as they go or deciding at a future date what their risk appetite should be.

> **"WE ARE WILLING TO ACCEPT FINANCIAL LOSSES, BUT DATA/PRIVACY LOSSES SIMPLY CANNOT BE TOLERATED.**

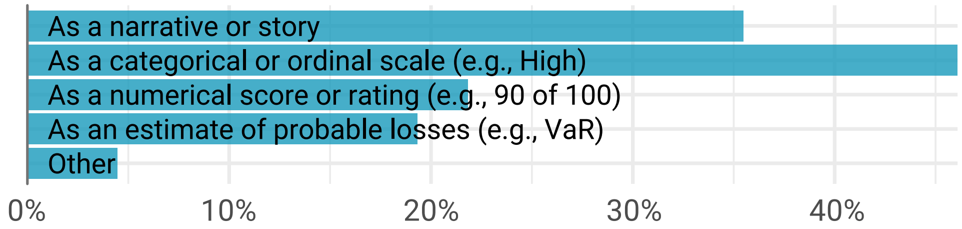
Of the respondents who said something about their organization's risk appetite, less than half were quantitative in nature. Qualitative descriptors like "very low" were most common, while some pegged risk appetite to external frameworks, as in this example: *"Our risk appetite follows the CMMI at the DEFINED level: processes are well characterized and understood, and are described in standards, procedures, tools, and methods."*

Of those that gave quantitative appetite statements, we observed a wide range of responses. Some came in the form of maximum acceptable loss. Some were expressed as a percentage of revenue. Others had probability and/or time components. Still others set certain qualifiers or stipulations for risk-taking. A few even claimed to have zero tolerance for cyber-related losses, though the viability of such a stance is unclear. In the information economy, some level of cyber risk is inherent to any business model

With respect to the question that began this Balance Point, only a handful of respondents gave comparable quantitative statements for both overall and cyber risk appetites. We can't discern much from so few data points, but it is worth noting that we saw no evidence that the stated tolerance for cyber-related losses was significantly different than for other types of losses.

Before leaving the topic of risk appetite, we should briefly address risk exposure. Put simply, this is an assessment of how much risk the organization is exposed to. Risk exposure can then be compared to risk appetite to determine whether the firm is operating within its "risk comfort zone." That assumes, of course, that these are comparable measures (notice we avoided saying "apples-to-apples" because that's too close to the actual "math" used in many risk assessments).

FIGURE 15: HOW IS CYBER RISK EXPOSURE EXPRESSED?



HOW DO YOU MEASURE UP?

> RISK APPETITE IS UNDERSTOOD AS QUALITATIVE RIGHT NOW: FULLY COMPLIANT WITH OUR REGULATORY FRAMEWORK AND AT LEAST AS GOOD AS THE AVERAGE PERFORMANCE OF OUR PEERS.

> RISK IS RATED IN CATEGORICAL OR ORDINAL TERMS. RISK APPETITE IS A BINARY WITHIN/OUTSIDE APPETITE. BOTH ARE SUPPORTED BY A NARRATIVE OF QUALITATIVE STATEMENTS AND NON-FINANCIAL METRICS.

> “WE WILL ACCEPT LOSSES OF UP TO $50-70M ANNUALLY FOR TAKING RISKS THAT ENABLE INNOVATION AND INCREASE COMPETITIVENESS.”

Part of the challenge here is the rather malleable notions of “risk” among security teams and Board members alike. The data, knowledge, and tools required to quantitatively analyze risk is a well-known and long-standing struggle for many organizations. We could elaborate further on reasons for that struggle, but a whole section in the 2017 Cyber Balance Sheet was devoted to this exact topic. We’ll refer you to that instead, and offer Figure 15 to refresh findings on how firms say they express cyber risk exposure in 2018. Hint: it’s still largely qualitative; the struggle is real.

WHERE TO FOCUS

A recent paper from Oliver Wyman recommends that an effective, measurable, and actionable cyber risk appetite should be:

- Risk-focused
- Reflective of risk strategy
- Cascaded (from top down)
- Leading (forward-looking)
- Actionable (drive decisions)
- Tailored to risk profile
- Measurable and monitored

> “THE TECH GUYS WANT TO MAKE THIS GEEKY WHILE THE PROCESS FOLKS ARE TOO THEORETICAL. THE BOARD DOESN’T KNOW WHERE THEY NEED TO START IN ORDER TO PUT A $$ NUMBER ON THIS.”

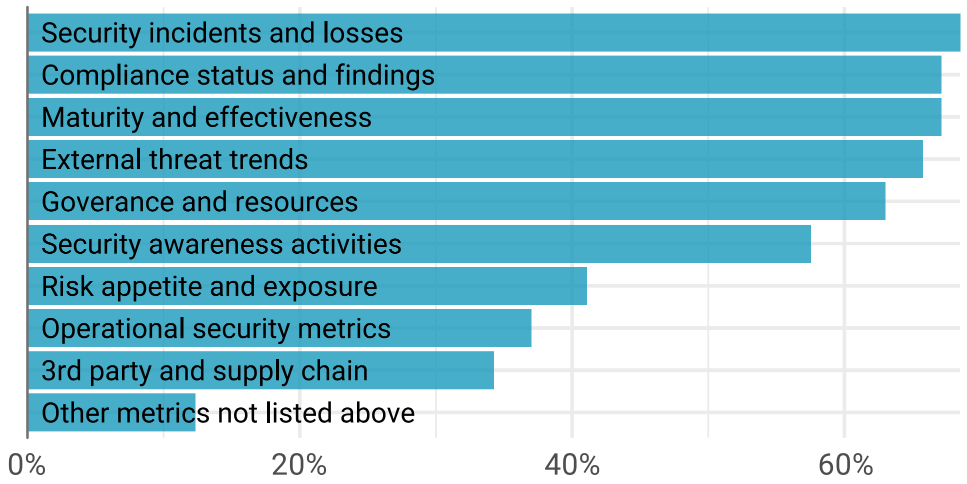
BALANCE POINT 4:

REPORTING CYBERSECURITY METRICS TO THE BOARD

Establishing a cyber risk appetite is one thing; satisfying directors' hunger to know where the organization stands relative to that appetite is another thing entirely. We examined board-level metrics for cybersecurity in our last study and witnessed the disparity that exists among security and business leaders when it comes to cyber risk communication.

In revisiting this topic, we drew heavily from the National Association of Corporate Directors (NACD) Handbook on Cyber-Risk Oversight for the categories of board-level metrics presented in Figure 16. These metrics are more fully described in Appendix A.

FIGURE 16: METRICS IDENTIFIED AS MOST OFTEN REPORTED TO THE BOARD



When asked which of these metrics were regularly reported to the board, respondents most frequently cited security incidents and losses. But compliance, maturity, and external threat trends rank within a point or two, and well within the margin of error. Suffice it to say that answering *"What's the danger and are we safe?"* sits high on the docket for board meetings. This likely relates to the low confidence and high anxiety among directors we observed in our last study.

> **IT'S DIFFICULT TO TRANSLATE SECURITY METRICS INTO BUSINESS TERMS. THE BOARD REPORTING PROCESS ITSELF TAKES MANY WEEKS AND ITERATIONS.**

The second tier on the reporting agenda looks to be ensuring the organization has the oversight, resources, and participation needed to successfully manage those topline items. Any weaknesses in the security culture or the organization or the quality of top-level support can quickly sap the strength of an otherwise solid defense.

Following on from the previous section, we can't help but notice cyber risk appetite and exposure sits among the least-reported categories. This is even more interesting because board members interviewed for last year's report ranked information on cyber risk posture as more important than anything else *(spoiler alert: we'll show in a later section that reporting cyber risk information helps enable board oversight)*.

> **“ BOARD-LEVEL CYBER REPORTING REQUIRES ‘DE-TECHING.’ METRICS USEFUL TO THE CYBERSECURITY ORGANIZATION ARE NOT APPROPRIATE FOR BOARD-LEVEL CONSUMPTION.**

The operational security metrics category falls near the bottom of Figure 16, and that's probably where it should be. A board member summed it up well: *“Nobody cares how many packets your firewall blocked. If security reporting doesn't reflect business goals, you're doing it wrong.”* It must be noted, however, that such metrics are very important for tracking the day-to-day status and activities of the security program and enabling CISOs to demonstrate areas of strength and opportunities for improvement. They just shouldn't be the main item on the boardroom agenda.

We did not ask about metrics pertaining to third parties last time, and so weren't sure what to expect for that category. Given the number of public incidents tied to vendors and the growth of services that monitor third-party risk, we're rather surprised to see it dead last. But deciding what it should replace in order to move up the list isn't easy. Plus, this category may be pushed down simply because not all firms operate large supply chains (or don't consider up/downstream risks).

Recall that our fourth research question asks how cybersecurity reporting varies across different types of organizations. The number of ways we sliced the data in pursuit of answers to that question borders on the absurd, but we will shield you from that tedium by summarizing what we learned in the “Noteworthy Distinctives” callout on the next page. We will also stick to the facts in those observations rather than speculate as to their reasons and meanings. But we heartily encourage you to do so!

> **“ AVOID THE DESCENT INTO TECHNOBABBLE AND IRRELEVANCE. BEST TO CONSIDER NOT WHAT THE ISSUE IS, BUT WHAT IT MEANS TO THE BUSINESS, TACTICALLY AND STRATEGICALLY.”**

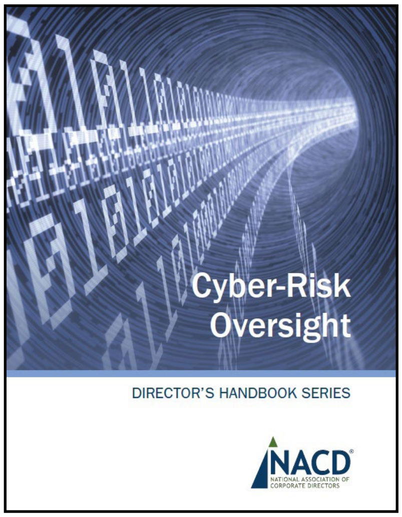
NOTEWORTHY DISTINCTIVES:

- Threat trends rise to #1 for financial services, yet fall to #9 (last) for communications & tech.
- For-profit companies report maturity metrics most often, whereas public sector and non-profits stress compliance.
- The previous statement also applies to larger vs. smaller firms.
- Highly-regulated firms put far more emphasis on governance and resource metrics.
- Organizations with established risk appetites crave cyber risk metrics in the boardroom. So do those that identify as risk-seeking.
- Firms that do not report on maturity and effectiveness may be making it harder on themselves.

WHERE TO FOCUS

We stand behind our guidance on this topic from last year: Metrics reported to the board should be tied to business-level outcomes supported by the security program. All parties should agree on the metrics, establish thresholds and goals, and understand what changes over time signify. Ideally, every metric and movement should have meaning that can be used to support management decisions.

THE NACD CYBER-RISK OVERSIGHT HANDBOOK


Cyber-Risk
Oversight
DIRECTOR'S HANDBOOK SERIES
NACD
NATIONAL ASSOCIATION OF CORPORATE DIRECTORS

Fortunately, those wishing to improve how cybersecurity is communicated to the board have a growing set of resources at their disposal. The NACD Cyber-Risk Oversight Handbook is a great place to start.

Per the NACD, board-level cybersecurity metrics should:

- Be relevant to the audience
- Be reader-friendly
- Convey meaning
- Be concise
- Enable dialogue

The NACD further encourages the use of charts and other visuals, trending metrics over time, peer/industry benchmarks, and relative performance indicators. We asked respondents which of these featured into their board reports and received the following results:

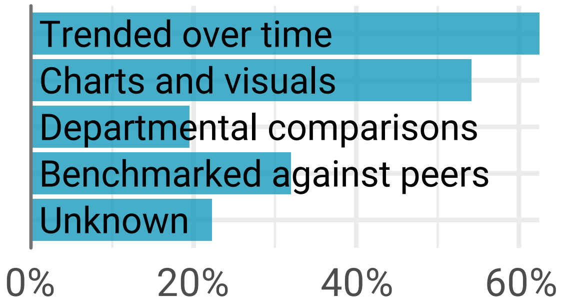


FIGURE 17: METRICS PRESENTATION

BALANCE POINT 5:

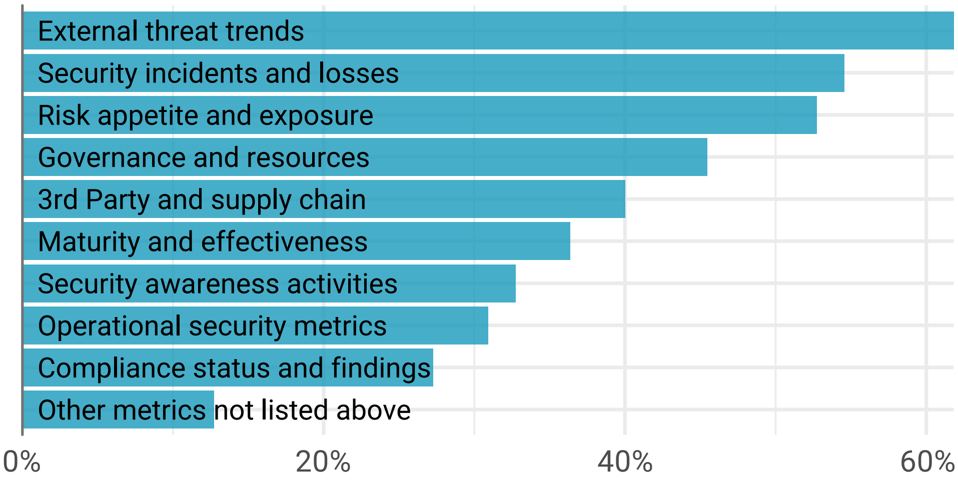
DRIVING DIALOGUE AND VALUE IN THE BOARDROOM

In addition to metrics most often reported in the boardroom, we took a cue from NACD to study the dialogue around these metrics. The aforementioned Director's Handbook says that cyber risk reporting should "above all, enable discussion and dialogue." We also attempt to measure the perceived value of these metrics. This is admittedly a subjective notion, but we asked respondents to identify metrics that have *"top value in terms of enabling board-level confidence and oversight for cyber security and risk."*

Input gathered from respondents on the top drivers of dialogue in the boardroom is captured in Figure 18. Based on the top three categories listed, we'd like to be a fly on the boardroom wall for those conversations. Maximum airtime is given to threats, incidents, and risk, with minimal discussion of operational minutiae and compliance — just like we like it! In all seriousness, though, it's quite interesting to see how the categories rearrange here.

FIGURE 18: METRICS IDENTIFIED AS TOP DRIVERS OF BOARDROOM DIALOGUE

Maximum airtime in the boardroom is given to threats, incidents, and risk, with minimal discussion of operational minutiae and compliance.

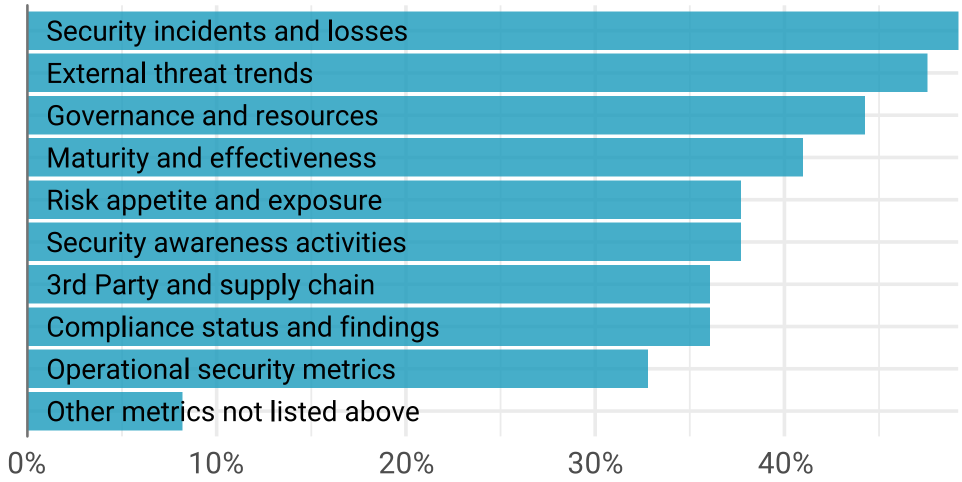


> **WE HAVE GOTTEN MANAGEMENT TO THE AWARENESS THAT CYBER IS SCARY, BUT NOT TO THE POINT OF UNDERSTANDING IT AND PLACING IT IN THE BROADER PICTURE OF RISK AND PRIORITIES.**

The value-based view of metrics in Figure 19 offers a slightly different outlook. Incidents and threat trends still top the list, but maturity metrics bump up and risk exposure slides down a couple notches. It's curious that risk would drive dialogue, yet yield comparatively less value. We can't help but wonder if this ties back to Balance Point 3 regarding how risk exposure is typically expressed. Perhaps the stories, scales, and shades of cyber "risk" presented to the board isn't very satisfying to a group of people accustomed to looking at risk more quantitatively and/or in a business context.

FIGURE 19: METRICS IDENTIFIED AS MOST VALUABLE TO THE BOARD

Boards appear to place high value on situational awareness (external and internal) and whether the organization is equipped and capable to deal with it all.



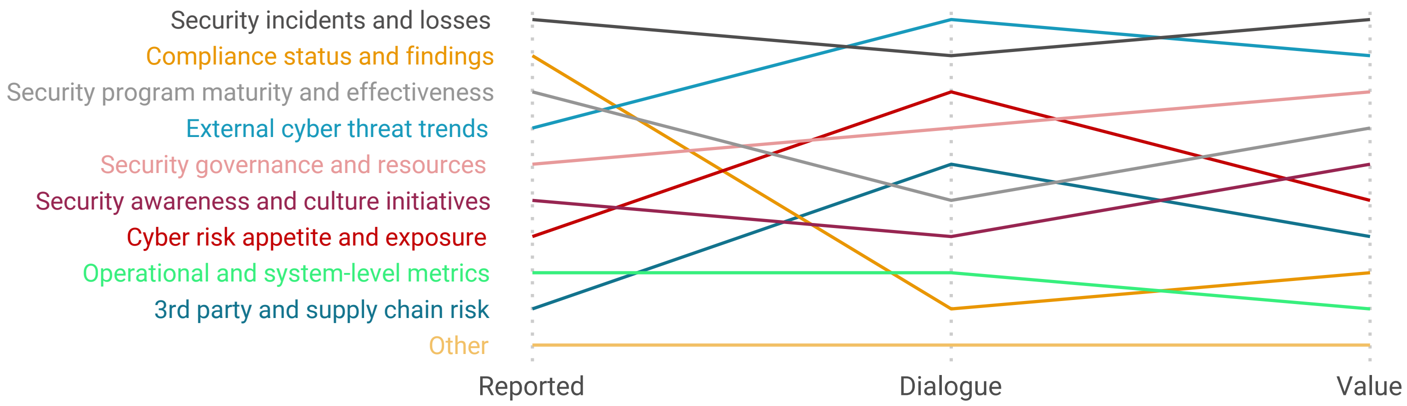
There are several other interesting shifts between Figures 18 and 19 (and Figure 16 from the previous section), but tracking them across multiple separate charts and pages is not an easy feat. To aid such comparisons, we present Figure 20 on the next page. It tracks how the ranking for each category of metrics changes across the reporting, dialogue, and value dimensions. Much could be pondered and postulated regarding Figure 20, but we will focus on metrics that appear over or under-reported relative to the dialogue and value they drive.

> WE HAVE FALLEN INTO THE TRAP OF PROVIDING TOO MANY TECHNICAL METRICS IN THE NAME OF SELF-JUSTIFICATION. BUT BECAUSE THE BOARD DOES NOT KNOW WHAT THESE MEAN FOR THE BUSINESS, THEY ASK QUESTIONS AND WE END UP WITH NOISE FEEDING ON ITSELF.

Compliance stands out in Figure 20 as having a particularly poor "return on reporting." Its ranking in the reported column is notably higher than for dialogue and value. That may be because showing what's been done is easier than answering the more important questions of whether it's enough and what should be done next.

External threats, cyber risk, and third party metrics look as though they may be under-reported based on their potential benefits in the boardroom. We've discussed the merits of these metrics already, so we won't do so here again. If they aren't on your reporting agenda, thinking about how to incorporate them may be time well spent.

FIGURE 20: COMPARISON OF HOW BOARD-LEVEL CYBERSECURITY METRICS ARE REPORTED, DISCUSSED, AND VALUED



WHERE TO FOCUS

Pay close attention to board reactions during cybersecurity reporting. What raises eyebrows? What prompts discussion (positive and negative)? What questions are asked? Why are they asked? What changes the tone and course of the conversation? It may be helpful to bring an observer to take notes.

NOTEWORTHY DISTINCTIVES:

- Governance metrics own the dialogue in risk-averse firms
- Risk-seeking firms place high value on awareness and operational metrics
- Private companies heavily discuss governance and third party metrics and put more value on awareness.
- Dialogue (and value, to a lesser extent) in SMBs centers on governance and operations
- Firms ranking cyber risk at/near the top of all risk types also rank it at/near the top for board dialogue and value.

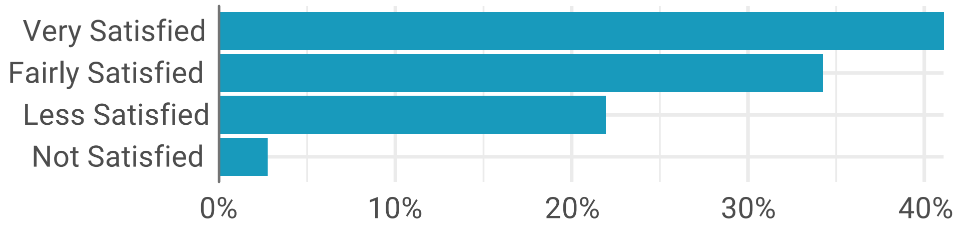
BALANCE POINT 6:

IMPROVING BOARD SATISFACTION AND CONFIDENCE

Reading between the (literal) lines in Figure 20 of the preceding section, gives the impression that the information most valued in the boardroom doesn't necessarily get the most attention. Two responses are common among humans from the boardroom to the playroom when their needs are not met: they become dissatisfied and/or lose confidence. We'll look at those responses in this section and, most importantly, what might be done to turn them around.

FIGURE 21: HOW SATISFIED ARE YOU WITH BOARD-LEVEL CYBERSECURITY REPORTING IN YOUR ORGANIZATION?

Overall satisfaction with board-level cybersecurity reporting rates fairly high...



According to Figure 21, overall satisfaction ratings are almost counter-intuitively positive. The highest proportion are "very satisfied" with security reporting and 3 out of 4 are more happy than not. This tracks with what we heard from both business and security leaders last year. It's almost as if there's a prevailing uncertainty about what "good" looks like, and so any information on cyber risk is seen as an improvement over nothing. Despite increasing focus over the last few years, board-level cybersecurity reporting is still a relatively immature discipline.

NOTES FROM THE FIELD

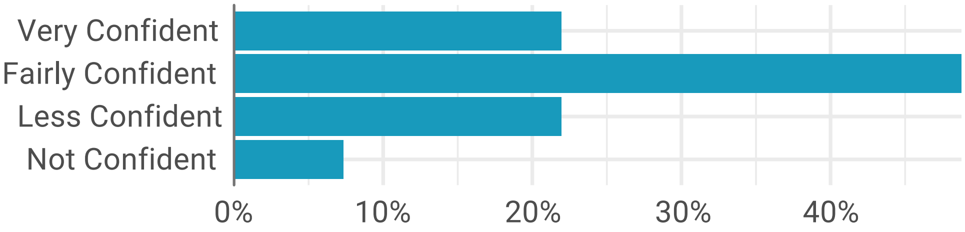
> “THE BOARD HAS NOT INDICATED THAT IT IS UNHAPPY; HOWEVER, I'M NOT CONVINCED THEY KNOW WHAT THEY TRULY WANT.

> “BASICALLY, THE BOARD WANTS TO KNOW IF SECURITY IS MANAGED OR NOT. DETAILED METRICS ARE GENERALLY INFORMATION OVERLOAD.”

That veneer of satisfaction, however, begins to chip away a little when the line of questioning turns to confidence in Figure 22. The largest contingent is now “fairly” rather than “very” confident, but the majority (72%) still lands on the side of confidence. This suggests business leaders might nod their heads in apparent approval during a cybersecurity status report, but retain deep-down concerns about what it all means and how they use that information to provide oversight to the business.

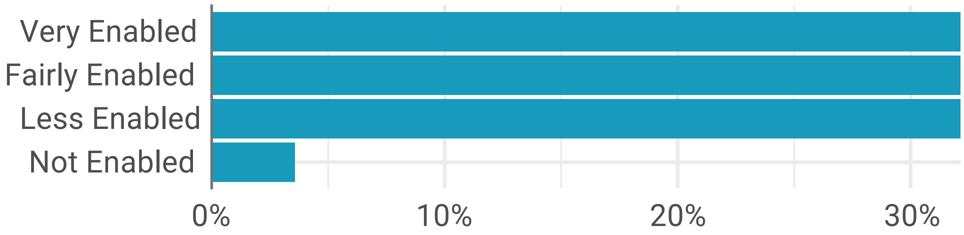
FIGURE 22: HOW CONFIDENT ARE YOU THAT YOUR ORGANIZATION IS EFFECTIVELY MANAGING CYBER RISK?

...but that satisfaction doesn’t translate directly into equivalent levels of confidence.



With respect to oversight, that is ultimately what board-level reporting — cyber or otherwise — should enable. So we asked directors and business leaders about their level of enablement and tallied their responses in Figure 23.

FIGURE 23: HOW ENABLED IS THE BOARD TO PROVIDE THE NECESSARY OVERSIGHT OF CYBER RISK FOR YOUR ORGANIZATION?



> “ BOARD MEMBERS WANT TO BETTER UNDERSTAND CYBER RISK, REQUIRING A SET OF METRICS GIVING A BROAD OUTLINE OF OUR POSTURE AND PROGRESS.

Comparing the figures above in progression gives the impression of a gradual erosion of confidence and enablement. "I'm satisfied, fairly confident, but not really enabled" seems to be the underlying sentiment. The majority of respondents still lean toward enablement, but the ratios are more balanced than in the figures above.

The question at this point is whether anything can be done to stop this erosion at the top. Do we see a link between certain metrics reported to the board and higher levels of satisfaction, confidence, and ultimately, enablement? We investigated that very question and a summary of what we observed is given in the callout below.

> **SIMPLE METRICS AND BENCHMARKING ARE CRITICAL TO GAIN CONFIDENCE.**

WHERE TO FOCUS

CISOs should consider asking for time once per year to review board-level metrics with directors and other business leaders to determine how effectively they promote satisfaction, confidence, and enablement. This session should be separate from regular reporting, and focus on how useful current metrics are (or aren't) to those tasked with making business risk decisions based on that information.

NOTEWORTHY DISTINCTIVES:

Satisfaction

- Firms claiming high satisfaction with board-level cybersecurity reporting were more likely to include maturity and incident metrics.
- Less satisfied organizations reported compliance and awareness metrics more than anything else.

Confidence

- The most confident organizations list threat trends and maturity metrics as #1 and #2 on the reporting agenda.
- Reporting risk metrics is the biggest relative difference between firms with higher vs. lower confidence levels.
- Less confident organizations reported compliance and incident metrics more than anything else.

Enablement

- Nearly all business leaders who say they are enabled have governance metrics reported to them. The data isn't sufficient to determine causation, but it is the only case where governance metrics are #1.
- Among those who claim to be "highly" enabled, all but one report cyber risk metrics. On the less/not enabled spectrum, only one firm reports risk metrics.
- Less-enabled firms seem to spend an inordinate amount of time discussing incidents in the boardroom. Maybe reporting on incidents is a good thing, but letting them drive the discussion is unwise?

BALANCE POINT 7:
ENABLING THE BUSINESS

The previous section identified objective factors that improve the board's confidence and ability to exercise oversight for cyber risk. Many security leaders also expressed a desire to more effectively enable the business at-large. We applaud that desire and want to do our part to support their endeavor. Below you'll find a suggested "path to enablement" for cybersecurity leaders constructed using insights and recommendations shared by respondents.

STEP 1: UNDERSTAND BUSINESS.

It's hard to enable something if you don't have a decent grasp of how it works. CISOs that lack a basic business background should consider pursuing an MBA or at least doing some weekend reading. Financial Intelligence by Berman and Knight is widely recommended, but ask around if you're not sure where to start.

> **"GO GET YOUR MBA AT NIGHT. LEARN CAPEX, DERIVATIVES, PROFIT AND LOSS, EBITDA, AND UNDERSTAND HOW A BUSINESS WORKS."**

STEP 2: UNDERSTAND *YOUR* BUSINESS.

Once you have a better foundation in general business terminology and processes, apply it to study your own company. Follow the money trail to understand key people, business units, products, and activities and then identify where information assets fall within all that. Learn about company strategy and important initiatives. Perhaps even consider mentoring or regularly meeting with a business leader.

> **"I WISH I'D PAID MORE ATTENTION TO HOW THE BUSINESS REALLY OPERATES. WHERE MONEY COMES FROM AND HOW IT'S SPENT."**

STEP 3: RELATE SECURITY TO THE BUSINESS.

Having framed out the core aspects of the business, you can now begin to consider how security fits into that picture. Evaluate the security roadmap in light of what you've learned and adjust accordingly. Be able to clearly articulate how security initiatives help the business and equip key members of your staff to do the same.

> **"FOR US, HAVING A SECURE PROGRAM IS THE COST OF DOING BUSINESS. THE ABILITY TO SHOW THIS IS THE DIFFERENCE BETWEEN WINNING THE SALE OR NOT."**

STEP 4: HELP KEY STAKEHOLDERS.

Get to know stakeholders across the business and ask what the security program can do for them. Helping make them successful will make you more successful as well.

> **"REACH OUT TO ALL STAKEHOLDERS AND ASK HOW YOU CAN HELP RATHER THAN HURT THEM. DON'T SIT IN YOUR SECURITY WORLD AND MAKE PROCLAMATIONS.**

STEP 5: SUPPORT BUSINESS DECISIONS.

Think of yourself as a decision supporter rather than a decision maker when it comes to things like business initiatives and risk acceptance. Replace *"We can't do that"* with *"If we do that, here are the types of risks we'll be exposed to and how we can work with you to reduce risk."*

> **"IT'S NOT SECURITY'S POSITION TO SAY 'NO.' WE'RE TO SAY, 'IF YOU DO THIS, HERE'S HOW TO LOWER RISK...' THUS, OUR ROLE IS ADVISING AND PARTNERING."**

STEP 6: SUPPORT REVENUE GENERATION

Endeavor to support revenue-generating activities and demonstrate that support to the board. If applicable, track customer interactions, contracts won, new products, etc. where security was a factor. Also ponder how security might support new streams of revenue (e.g., turn data into an asset rather than a risk).

> **"IN ANY COMPANY, THERE'S ONE SIDE THAT GENERATES REVENUE AND ANOTHER THAT'S GEARED TOWARD REMOVING RISK. WHILE SECURITY IS A DIRECT ENABLER IN SOME COMPANIES, IT IS OFTEN NOT SEEN AS ONE."**

The upshot of all of these steps is culture. The CISO's job based on these Balance Points should be to promote the adoption of safe and healthy practices that enable all employees, vendors, clients, and partners to operate with eyes wide open to the risks that they are taking with invisible information assets.

CONCLUSION

Thank you for taking the time to read our report. We hope it provides food for thought and action as you face the many challenges addressed by this research. To facilitate that, we conclude with a brief recap of the research questions we set out to explore and what we learned about them.

RQ1. HOW IS CYBER RISK PERCEIVED RELATIVE TO OTHER TYPES OF RISK? WHAT FACTORS ALTER THIS PERCEPTION?

Most respondents rank cyber risk in the upper tier of risks they're dealing with across the organization. Contrary to expectations, we did not see a pattern among those who place it toward the bottom. If there's a simple answer to *"If you're this and that, you don't/do care about cyber risk,"* we didn't find it.

RQ2. WHAT CYBER RISK INFORMATION IS REPORTED TO THE BOARD? WHAT DRIVES DIALOGUE AND VALUE?

Not surprisingly, board-level cybersecurity reporting appears to focus on threats and defenses. But we also learned that the metrics most often reported aren't necessarily the same ones that foster discussion and deliver the biggest value in the boardroom. Compliance metrics, for instance, rank #2 in terms of reporting, but fall to the bottom of the list for dialogue and value.

RQ3. HOW IS CYBER REPORTING VIEWED BY THE BOARD? WHAT DRIVES CONFIDENCE AND SATISFACTION?

Most boards are not vocally dissatisfied with current cybersecurity reporting, but we suspect they simply may not know what to ask for instead. There's some evidence that going beyond compliance to report on the maturity and effectiveness of the cybersecurity program could improve board-level satisfaction and confidence. Reporting on cyber risk appetite and exposure is another area where we saw a noticeable differences in confidence levels.

RQ4. HOW DOES CYBER RISK REPORTING — AND RECEPTION — VARY ACROSS ROLES AND ORGANIZATIONS?

It's clear that cybersecurity professionals and business executives have different views on cyber risk reporting. But it is far less clear how those differences apply to organizations. Even similar types and sizes of firms varied widely in how they perceive, measure, report, and manage cyber risk. We believe a better understanding of these subtleties is important to unlocking how cybersecurity programs influence and support the business.

> **SMART RISK TAKING REQUIRES GOOD RISK DATA, SO WE COMMUNICATE FREQUENTLY ABOUT RISKS WE ARE SEEING IN THE BUSINESS, GEOGRAPHY, AND INDUSTRIES WE SERVE.**

ACKNOWLEDGEMENTS

Focal Point and the Cyentia Institute would like to thank the more than 150 CISOs, CIOs, CEOs, CFOs, CROs, CAEs, and board members that participated in the 2018 Cyber Balance Sheet Report. As the Report itself demonstrates, there is no shortage of demands on your time. We are immensely grateful of your willingness to set aside some of that valuable time to contribute to this research.

The researchers also wish to thank the American Institute of Certified Public Accountants (AICPA), the FAIR Institute, the National Association of Corporate Directors (NACD), and the CFO Leadership Council for their valuable support of this project. We hope your memberships find the research useful and relevant.

And lastly, the Cyentia Institute would like to recognize and thank Dr. Christophe Veltsos for acting as a research advisor on this project.

INTERESTED IN CONTRIBUTING?

Our team is always looking for cyber security leaders and executives to participate in our research. If your interested in contributing to next year's report or future Cyber Balance Sheet projects, shoot us an email at contribute@cyberbalancesheet.com and we'll be in touch.

APPENDIX A:
DESCRIPTION OF METRICS CATEGORIES

EXTERNAL THREATS

Updates on the evolving cyber threat landscape, including emerging threats, intelligence updates, major incidents, etc.

GOVERNANCE AND RESOURCES

Status and updates on security planning, projects, budgets, spending, procurement, staffing, etc.

MATURITY AND EFFECTIVENESS

Assessments regarding the state and strength of security capabilities relative to threats facing the organization.

COMPLIANCE STATUS AND FINDINGS

Reports on the organization's compliance (or non-compliance) to security-related regulations and standards.

RISK APPETITE AND EXPOSURE

Statements about the level of risk the organization is willing to accept and assessments of current exposure to cyber risk.

SECURITY INCIDENTS AND LOSSES

Metrics on internal security incidents, breaches, attacks, outages, policy violations, abuse, etc.

SECURITY AWARENESS ACTIVITIES

Updates on security training programs, phishing trials, staff compliance with internal policies, etc.

OPERATIONAL SECURITY METRICS

Metrics such as system or application vulnerabilities, patch levels, pentest findings, incident detection and response timeframes, etc.

THIRD PARTY AND SUPPLY CHAIN

Assessments of the cyber risk posture of suppliers, vendors, customers, and other value chain partners

CYBER

BALANCE SHEET

cyberbalancesheet.com