CYBER BALANCE SHEET

THE 2017 REPORT

Sponsored by FOCAL POINT DATA RISK

FOCAL POINT
DATA RISK

The Cyber Balance Sheet Report is sponsored by Focal Point Data Risk.

In addition to this Report, Focal Point sponsors and hosts the Cyber Balance Sheet Summit, an exclusive half-day event for Board members and select corporate executives, focusing on the cyber issues that matter most to business leaders. The 2017 Summit was held at the Nasdaq MarketSite in New York City on January 27. Insights from the Cyber Balance Sheet Summit were instrumental in the development of this report.

About Focal Point Data Risk

Focal Point is a risk management firm 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 cybersecurity, identity governance, data privacy and analytics, and hands-on training services. By integrating these services, we provide our clients with the flexible support they need to leverage, analyze, and protect data across any part of their organization. Simply put, Focal Point is the next generation of data risk management.

Visit focal-point.com for more.

CYENTIA®
INSTITUTE

The Cyber Balance Sheet Report was independently researched by the Cyentia Institute.

The Cyentia Institute is a research-services firm that exists to advance cybersecurity knowledge and practice through use-inspired, data-driven research. Cyentia curates and publishes research for the community, partners with other organizations to create compelling publications, and helps enterprises turn complex security data into confident strategic decisions.

Visit www.cyentia.com for more.

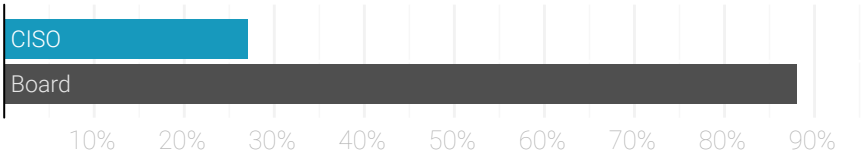
ABSTRACT

“The things cited by Board members as most critical fell dead last among CISOs.”

This innovative study prepared by the Cyentia Institute breaks down walls between cybersecurity leaders and Boards of Directors. Data is often said to be the lifeblood of the company; yet, there is immense frustration at how risks to that information are measured, mitigated, and communicated across the enterprise. As the financial, regulatory, and legal stakes of data breaches and disruptions rise, leaders at all levels must come together to protect and further the business.

Scores of in-depth interviews reveal six Balance Points where Chief Information Security Officers (CISOs) and Board member viewpoints are prone to diverge. Our findings show that even basic questions on the value of cybersecurity show little consensus; things cited by Board members as most critical fell dead last among CISOs! Given that, of course, key performance indicators (KPIs) sought by each group differed widely as well, inevitably resulting in diminished confidence at the top.

Who values business-level metrics for cybersecurity?



The chart above highlights the dilemma from differing perspectives. 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 more equitable path forward is needed. We conclude the report by introducing the concept of a Cyber Balance Sheet, which borrows familiar terminology of assets and liabilities to improve communication and consensus around cyber risk.

BALANCE POINT

A specific point of differentiation in the way Board members and security teams think, talk, or make decisions about cyber risk. This report examines six of the most prevalent Balance Points of 2017.

CEO PERSPECTIVE

“The ability to express what you get for your money in an impactful way is a critical prerequisite to building confidence in the value of a cybersecurity program.”

- John Madelin
CEO, Reliance acsn

CONTENTS

INTRODUCTION

"Cybersecurity is a Board-level issue."

We've heard that phrase, or some form of it, for years now. There was a time when it was a bit of wishful thinking promulgated by security staff who wanted to get the attention of business leaders. Few would argue now that they are getting what they wished for. Indeed, information assets now comprise the majority of a company's value, and the barrier between business and security processes erodes ever faster (if it even still exists). Board members can be held personally liable for breaches and disruptions impacting the companies they govern, prompting them to demand a defined level of accountability security leaders and management often struggle to provide.

Unfortunately for all involved, the critical, strategic area of cybersecurity measurability has received far less attention from researchers than threats, vulnerabilities, and related operational matters.[1] Seeking to fill that void, the Cyentia Institute and Focal Point produced this study. Our research goals were to gather perspectives, characterize key issues, identify possible solutions, and draw security and business leaders together through greater shared understanding and purpose.

Based on these goals, one-on-one interviews consisting of mostly open-ended questions were selected as the most appropriate research method. Due to the inherent difficulty of reaching the target subjects (security executives and Corporate Directors), we did not believe obtaining a random sample was realistic. We opted for a "snowball" sampling technique, in which we started with known associates and asked them to introduce us to other participants. A focus group session was also used to collect data during the Cyber Balance Sheet Summit at the Nasdaq MarketSite in New York City. When schedules were not conducive to setting up an interview, questions were provided via email or web form.

Using these methods, we collected information from more than 50 CISOs and security directors ("CISOs" from now on), 25 Corporate Directors, and 10 subject matter experts who work with these two groups. About 75 attended the Summit and contributed supplemental information in the form of panels, comments, etc. Interviews typically lasted 30-45 minutes and were conducted by a Cyentia Institute representative who took detailed notes. Those notes along with information collected in the ways described above form the corpus for the analysis that follows.

While this is classic qualitative research, we wanted to offer some data-driven findings (though in the form of relative frequencies and rankings rather than precise measurements). We accomplished this by analyzing interview notes for common themes or categories and then coding each response accordingly. For instance, a theme of security guidance emerged from talking to interviewees about the value of cybersecurity to the business (see Balance Point 1). Someone said, "Help the business understand security," which we coded as security guidance. All counts and percentages shown in this report were derived in this manner. Appendix B contains definitions for all categories used.

We want to offer our sincere thanks to all who participated in this research. Volunteering 30-45 minutes of one's time is no small matter for anyone, but is particularly generous for executives, who have notoriously hectic schedules. We deeply appreciate it and hope you feel that time was well spent after reading this report.

- Wade Baker, Co-Founder of the Cyentia Institute

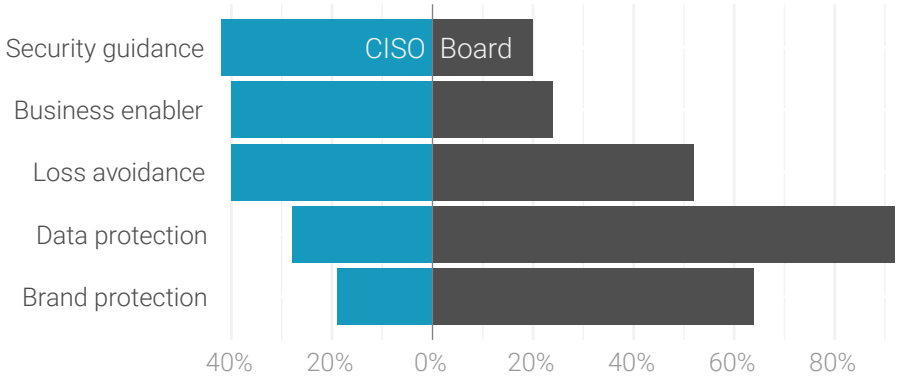
[1] Examples of reports on this topic include *Cybersecurity in the Boardroom* from NYSE Governance Services/Veracode and *How Boards of Directors Really Feel About Cyber Security Reports* from Ostermann Research/Bay Dynamics.

BALANCE POINT 1

THE VALUE OF CYBERSECURITY

We began with a broad, yet pointed question about the value of cybersecurity to the business. After all, if there isn't alignment here, then everything else will be an uphill — and ultimately losing – battle. Ostensibly, the most straightforward answer would be some form of "protecting company data." But what exactly does that mean in an age where intellectual property (aka the "crown jewels") makes up the majority of company value? The CISOs and Board members we interviewed had a variety of thoughts on that, but most fell within the broad categories shown in Figure 1.

Figure 1
What is the primary value of cybersecurity to the business?



Being responsible to stockholders and stakeholders of the companies they govern, Boards are well-versed on the topic of value and keenly aware that valuation and information are increasingly intertwined. As a testimony to this awareness, Board members cited brand and data protection as the cybersecurity function's primary responsibility to the business. CISOs, on the other hand, mentioned these two pillars far less often, which certainly seems counterintuitive.

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."

Figure 1

CISOs and Board member perspectives differ on security's main role. The Board wants to avoid data breaches and brand damage. CISOs want the same, but say guiding and enabling the business is their biggest value add.

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."

Upon further reflection and discussion, this may not be as much of a discrepancy as it appears, and likely stems more from differences in perspective and priority than any strong difference of opinion. CISOs of course know that protecting data lies within their purview, but they're also pressured on various fronts to demonstrate how that helps the bottom line. And so they've learned to position security as a business enabler rather than a cost center whenever possible. Undoubtedly the Board would be thrilled if that came to pass, despite explicitly listing it as one of security's primary values far less often. But data and brand protection represent more immediate security-relevant concerns to their mind. As one Board member put it:

"My top concern is the legal and business implications of a breach on the company overall because it is a Director-level liability."

Is it a sign of maturity or wishful thinking that business enablement tops loss avoidance and data/brand protection in the minds of CISOs? Perhaps both, and that may not be a bad thing. Stretch goals can be helpful, and many expressed a desire for security to offer the business more than a hand slap and a firm "no."

It is rather telling that security guidance was the most common value identified by CISOs. This is likely due to the difficulty they report in interacting with the Board on security matters. You'll see this important topic re-emerge in Balance Points 2 and 6.

Overall, these five categories cover security's value across the technical-business spectrum. Delivering and conveying that value proves more challenging, however, and we'll hit that head on in the next Balance Point.

CISO PERSPECTIVE

"We're able to understand infosec risk faced by the organization, make sure we're managing those risks, and articulate it all to the business."

BOARD PERSPECTIVE

"CIOs and CISOs often talk about what they want their jobs to be. The Board talks about what their main job should be: to protect the business and our liability."

FINDING THE BALANCE

Boards should take an active role in clearly establishing what the business needs from the security program. No one should assume this is obvious or shared by all stakeholders. If direction is not forthcoming, CISOs should initiate this discussion as soon as possible. Both parties should agree on what successfully providing this value looks like and what the Board expects in terms of assurances to that end. This will be of immense help to CISOs in delivering and conveying that value going forward. It is also a good step toward the U.S. Cybersecurity Disclosure Act of 2017, which would require public companies to provide information on the cybersecurity expertise of the Board relative to the needs of the company.

BALANCE POINT 2

CONVEYING SECURITY'S VALUE

Following from the previous section, it's not surprising that the majority of CISOs struggle to adequately convey the value of security to the broader business/Board, as Figure 2 reveals. When asked to elaborate on this challenge, they gave a host of reasons from which we identified several recurring factors.

Figure 2
Do you find it easy or hard to convey the value of security?

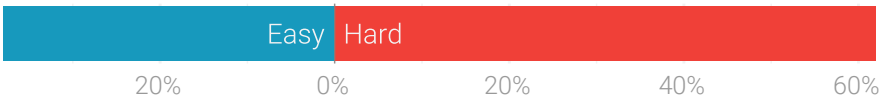
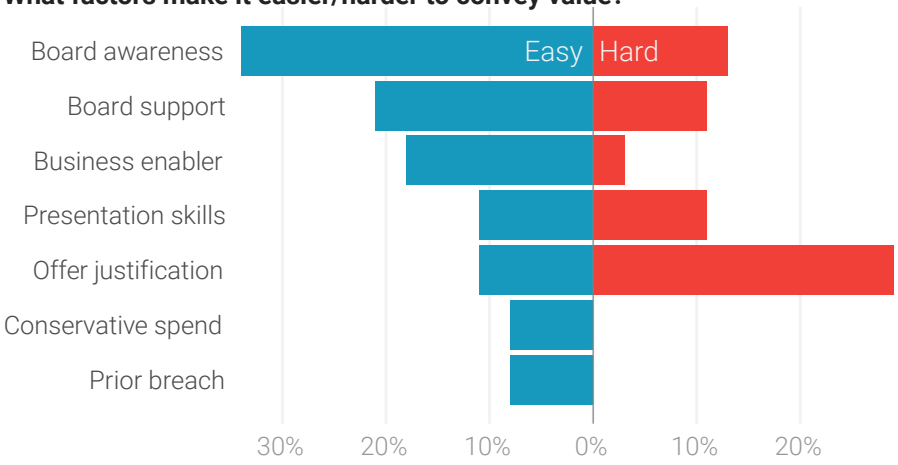


Figure 3
What factors make it easier/harder to convey value?



Per Figure 3, awareness and justification are the two extreme factors that seem to make or break the task of conveying value. Interestingly, the first ties back to Balance Point 1, where CISOs saw their primary value as providing security guidance. It certainly makes sense that having a security-conscious Board sets the tone at the top and makes the CISO's job easier, while the absence of that security awareness can have disastrous effects.

Several interviewees said the media was both a blessing and a curse in terms of raising awareness:

CISO PERSPECTIVE

"It's easy to relay value at a high level. The difficulty comes when you discuss specific activities."

Figure 3

Strong Board awareness and support make the CISO's job of conveying value much easier. They often find it hard, however, to adequately justify their programs to the Board. What and how they present can make or break their case.

"On one hand, the dangers of poor security are now front page news, which helps garner attention and support. Unfortunately, the press often hypes the wrong things, meaning I spend as much time saying, 'Don't worry about that,' as I do saying, 'We should worry about this.'"

Many security leaders find justifying their needs, plans, and progress to the Board a hard prospect, and this causes all manner of downstream difficulties. One CISO described this dilemma well:

"The Board has no appetite for any breaches. At the same time, I can't get them to spend the money necessary to prevent them. Hence the misalignment."

For many others, the disconnect is a type of language barrier. Still more cite insufficient evidence and metrics. All struggle with the conundrum of "proving a negative" that is inherent to security management:

"It's difficult to articulate why more money is needed when we haven't seen major incidents or impacts."

On a related note, presentation methods are depicted in Figure 3 as cutting both ways. CISOs who have solved the mystery of presenting to the Board say it makes their job a lot easier. Those who haven't, say the opposite.

"I always wondered what the disconnect was and then I realized the challenge was presenting security info in business terms. From that point on, I began looking at security goals in the context of business objectives."

Looking again to Figure 3, Board support is another balanced factor; having or lacking it can make all the difference. CISOs stepping into post-breach roles mentioned having the Board's backing from day one in the form of awareness, adequate budgets, political support, etc. Those without that luxury said it can be earned in other ways. For example, several mentioned that a conservative approach to planning, spending, and managing expectations helped earn the Board's trust. We share tips on winning support while *in* the Boardroom in Balance Point 6.

FINDING THE BALANCE

As stated previously, CISOs must first understand what the Board values. Infrequent and indirect contact with the Board can make this difficult, but CISOs should stress the importance to the business and use it as an opportunity to open a dialogue outside the Boardroom. Then they should use that information to orient the security program toward delivering and demonstrating that value. Boards should be cognizant of the challenges faced by CISOs and provide the necessary direction and feedback to help make them — and therefore everyone — successful.

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."

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."

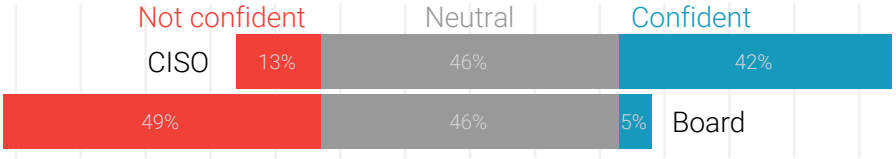
BALANCE POINT 3

ASSESSING POSTURE & PRIORITIES

Recall from Balance Point 2 that CISOs were having tremendous difficulty offering justification to the Board regarding the status and direction of the security program. There are several aspects to that challenge, the first of which is understanding how security posture, progress, and priorities are assessed.

However, before diving in, it's worth examining the disparity we uncovered between CISOs and Board members with respect to their confidence in the effectiveness of the security program. Per Figure 4, very few CISOs have doubts on that topic and about half give a thumbs up. Board members appear decidedly more skeptical; most of them express something less than confidence in the program.

Figure 4
Are you confident with the security program's effectiveness?



Given that difference of opinion, the obvious question is why this lack of confidence exists. Based on our discussions with both groups, we believe these notions of confidence and justification go hand in hand. Confidence at the Board level is driven by consistently delivering on promises and projections, and inadequate evidence from CISOs to that end unerringly leads to doubts among Board members. This seems to hold true even when the security program itself is otherwise in great shape.

But before credible justification of security posture and priorities can be provided to the Board, it must be collected by and for the program itself. According to Figure 5, the most common means of doing this is to evaluate against external standards and frameworks from entities like NIST, ISO, and FFIEC. For many, compliance with a particular standard is required. Others have the option to choose one that best fits their needs. Many juggle several of them across different business units and regions. Either way, assessment (at a basic level) involves identifying and filling gaps in requirements.

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."

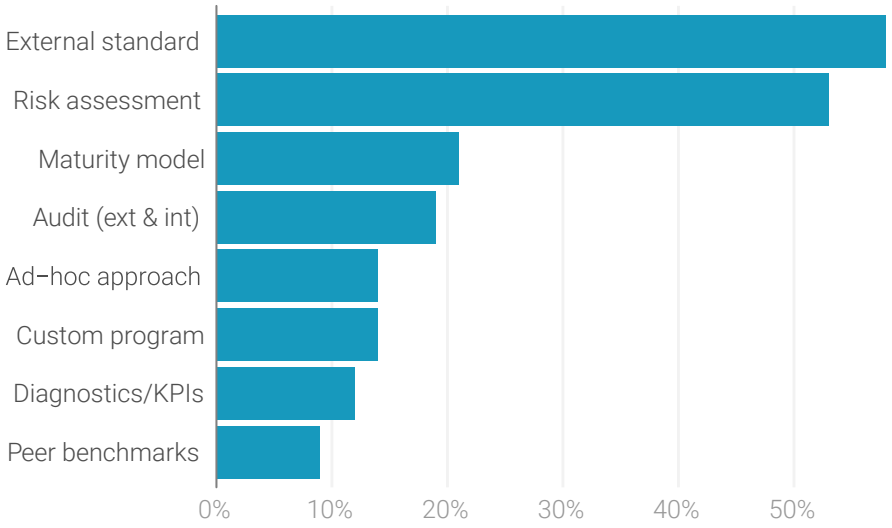
Figure 4

Very few CISOs have doubts about the efficacy of their program and almost half give a thumbs up. Board members appear decidedly more skeptical; most of them express something less than confidence in the program.

A common complaint levied against security standards is they measure adherence rather than effectiveness. Another gripe is the checklist approach doesn't offer much help in prioritizing what to check off next. These are valid points, and one of the many reasons risk assessments are commonly used alongside external frameworks. We won't go into what is meant by the use of the term *risk* here (see Balance Point 5 for that); we'll simply note that using some form of risk assessment is common. At a minimum, risk-based approaches seek to assess and address shortcomings based on their relative criticality.

Reported usage of the remaining methods listed in Figure 5 falls off relatively quickly. Aside from a wholly *ad-hoc* approach (e.g., "we pull in SMEs and let them argue it out"), these typically support or validate primary methods based on external standards or risk assessments. In the next Balance Point, we examine the types of metrics produced by these assessment methods.

Figure 5
How do you assess security posture and set priorities?



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."

Figure 5

Following external standards and conducting risk assessments are the most common means of evaluating security posture and priorities. The rest of the methods in Figure 5 typically supplement these two.

FINDING THE BALANCE

Knowing and showing the difference between the concepts of adherence and effectiveness are important. The Board's confidence isn't based on where the security program stands on a list of to-do's as much as whether it's standing strong in the face of material weaknesses to the business and headed in the right direction.

BALANCE POINT 4

FINDING MEANINGFUL METRICS

"If you can't measure it, you can't manage it" has long been a common phrase among proponents of metrics in many business domains. But those same people also know that not everything you can measure matters for management. Finding meaningful security metrics is particularly hard given the nature of the field and undoubtedly lies at the root of many problems discussed in previous Balance Points.

Figure 6 (next page) lists common metrics identified by interviewees as important and pounds home the message that "meaningful metrics" is a matter of perspective. The blue bar identifies metrics that CISOs find most useful for keeping tabs on the security program. The dark gray bar shows what Board members would value the most. The shaded region behind the bars corresponds to what CISOs say they currently report to the Board. The figure reveals several interesting insights.

At first glance, the disparity among CISOs and Board members regarding risk posture is rather shocking. Though the fact that CISOs report risk metrics to the Board more often than anything else does suggest they are aware of that disparity. Keep in mind that these findings do not imply CISOs don't track risk posture; it just seems their go-to metrics are more in line with day-to-day operations like system defects and security events/incidents.

Peer benchmarks show a similar pattern: Boards want them, but CISOs much less so, though they do make an effort to report them up. One issue here might be the historic difficulty in finding reliable apples-to-apples comparisons regarding security posture. Reversing that pattern are asset metrics. Boards are normally very focused on a company's assets, but those in view here are technical in nature and thus more relevant to CISOs who must protect them.

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."

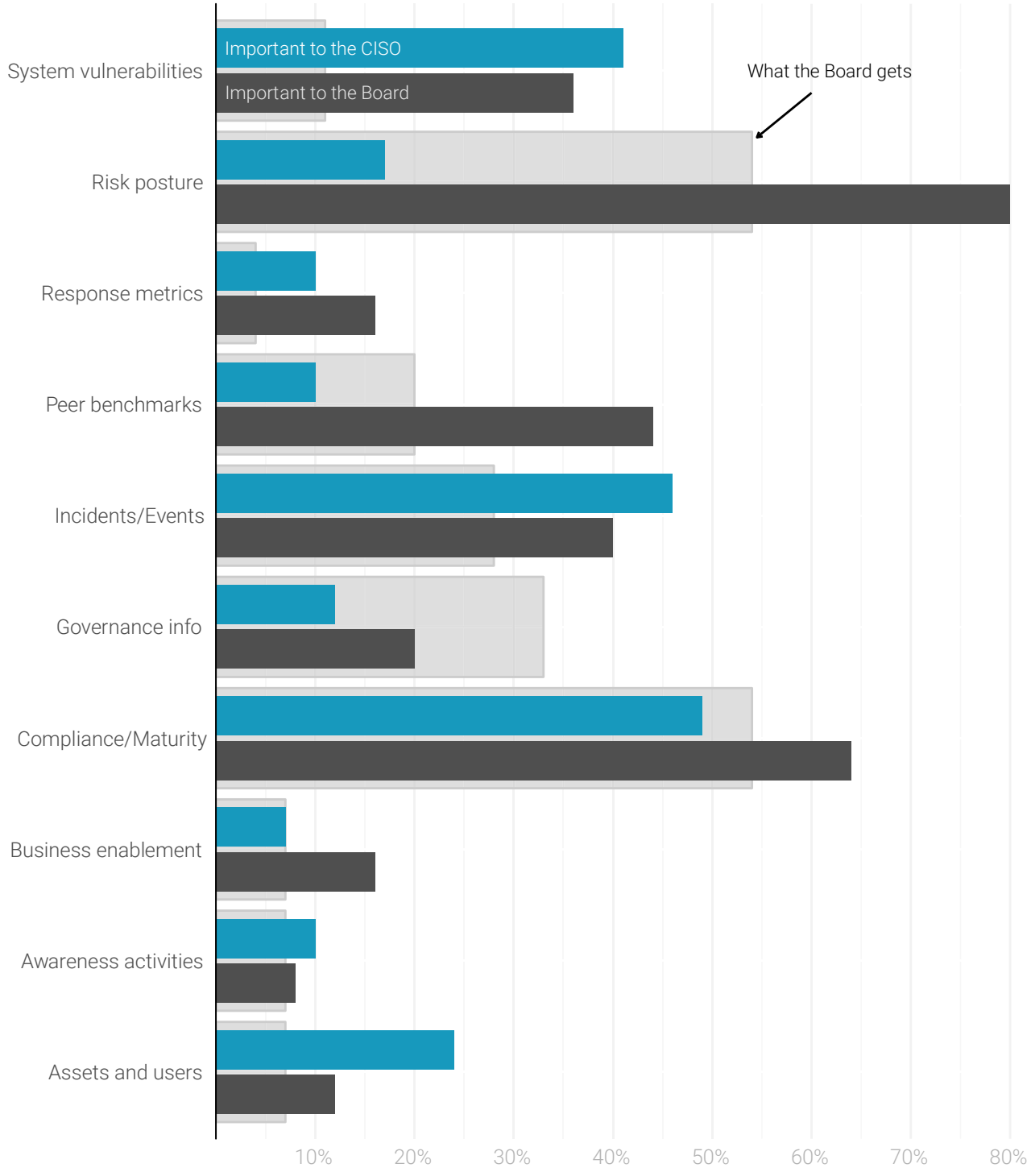
BOARD PERSPECTIVE

"Nobody cares how many packets your firewall blocked. If security reporting doesn't reflect business goals, you're doing it wrong."

THE METRICS MINEFIELD

MAPPING THE CONVERSATION

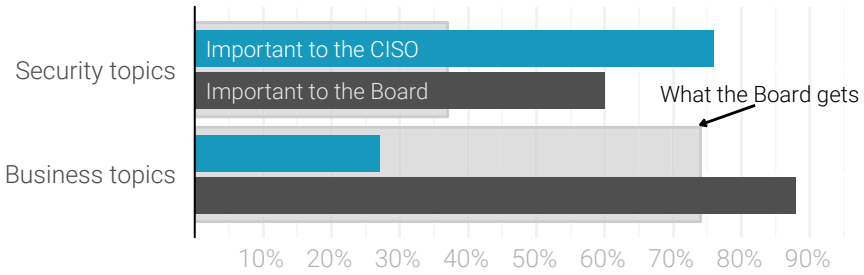
Figure 6:
What metrics do CISOs rely on most? What's reported to the Board? Which do Board members value most?



An interesting observation is that governance is the sole over-reported category in Figure 6. One wonders if things like spending, staffing, and projects are reported more out of ease of measurement than Board-level usefulness.

Figure 7 offers a simplified view of Figure 6. The more detailed metrics categories from Figure 6 are distilled down to contrast security topics against business topics. Perhaps surprisingly, CISOs and Board members aren't terribly far apart on what they'd like to see presented in terms of security topics. The difference between them is very obvious for business topics, however, and reinforces the key challenge. But the figure does offer a ray of hope. What is actually reported represents a compromise of sorts: CISOs are clearly increasing the supply of business-level metrics (especially cyber risk) to meet the demand from the top. A worthy aspiration to be sure, but interviewees say the difficulty lies in the execution. The next two Balance Points offer some clarity and help in that pursuit.

Figure 7
The quest to align the conversation



FINDING THE BALANCE

It's OK to have different metrics for different audiences and purposes, but understand what's what. 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 has meaning that can be used to support management decisions. The National Association of Corporate Directors (NACD) publishes some guiding principles for Board-level metrics, which those responsible for preparing and delivering them should review.

CISO PERSPECTIVE

"For each finding in the assessment, there is a security initiative. The list is long...too much to do in this lifetime."

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?"

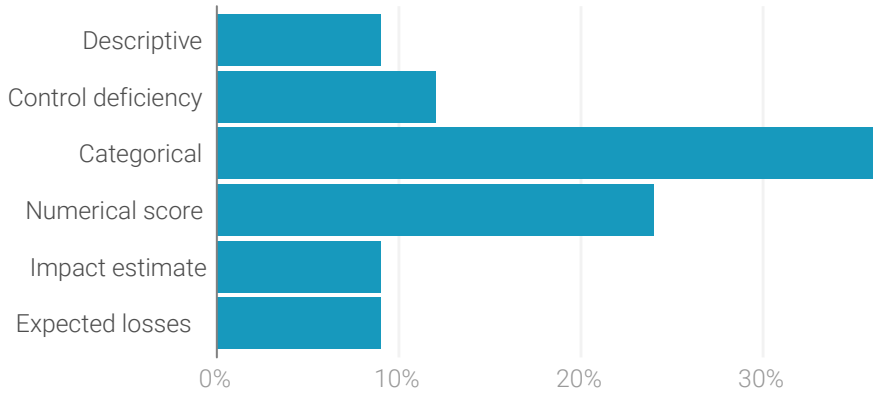
BALANCE POINT 5

MEASURING & EXPRESSING RISK

Risk. It may seem like a simple four-letter word with a widely understood definition firmly ensconced in generations of practice. Boards are very accustomed to the concept of enterprise risk management (ERM), and discussing the financial, strategic, and operational risks to the firm is standard Boardroom fare. Opening up a discussion on cyber risk, however, is a lot like Forrest Gump's box of chocolates — you never know what you're gonna get. But we can at least describe what we are getting since previous sections show Boards have a real sweet tooth for risk.

We approached our talks with CISOs on this topic very openly to learn how they were measuring risk without leading or tainting their explanation. We could write a full report based on those descriptions alone, but our current endeavor is to distinguish them as qualitative vs. quantitative vs. something in between. After analyzing the discussions, we landed on the labels given in Figure 8.

Figure 8
How is cyber risk measured in your organization?



It's easy to see that not many measure risk in terms of financial losses expected over a given timeframe. A few more show loss figures, but base them solely on the possible impact of events without regard to probability. Another small contingent rejects all that mathy stuff, opting for a purely descriptive accounting of risks. Most approaches fall somewhere between "words" and "dollars," using some form of categorical rating or numerical score as a proxy for risk.

CISO PERSPECTIVE

"There's a language problem with risk vs. risks. Many sit around a table thinking of what could go wrong and then think of controls to mitigate those risks. They call this risk management but it's not."

BOARD PERSPECTIVE

"Many Boards understand risk management and see that as their job. If the CISO can be comfortable in that environment, then s/he will have greatest chance of success."

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."

One respondent candidly admitted:

"We're doing all the things Jack Jones says you shouldn't do.[2]"

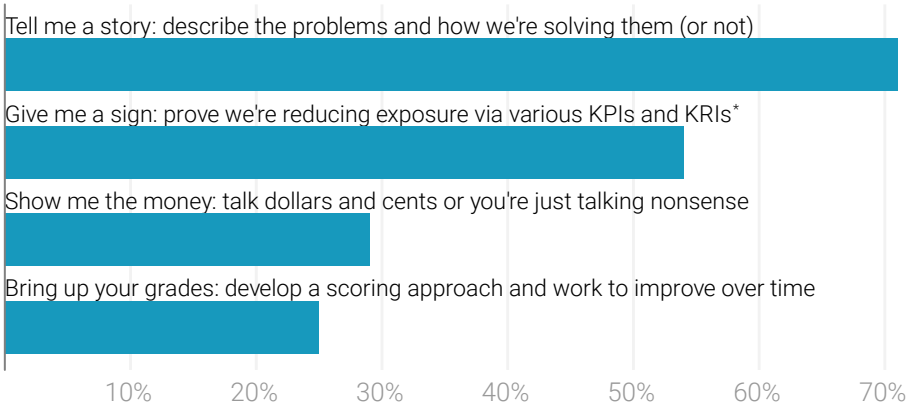
We want to tread lightly because the whole qual-quant risk debate involves strong opinions on both sides. In a rather ironic example of that, we did back-to-back interviews with two CISOs who had this to say:

- **"There is an edict from senior management that we don't report dollars at the Board-level."**
- **"Presenting risk in financial terms is what the Board wants and that's the goal we've set."**

There's no way we're going to bridge that divide here, but another interviewee showed there is some middle ground: **"Thinking in proper risk terms is essential, but quantifying in dollars per year depends on data quality and capability maturity."**

Rather than take sides on this issue, we decided to ask Board members how they'd like to see cyber risk expressed. Their input is below, listed in order of preference:

Figure 9
Board member preferences for ways to express risk



We can't help but notice things topping the CISOs' list (categorical ratings and numerical scores) align with "bring up your grades," which sits at the bottom of the list for Board members.

FINDING THE BALANCE

Ultimately, how risk should be expressed is a product of Board preference and organizational maturity. If yours isn't ready for quantification, begin by using proper terminology and logic in your qualitative descriptions of risk. Experience shows that Boards fed mostly words about risk will eventually begin asking questions that require numbers, and likely dollars, to adequately answer. When it comes to that, there are some good resources out there to help CISOs and their staff meet that need.[3]

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."

Figure 9

"Tell me a story and then back it up with a few numbers." That's pretty much the consensus from Board members on expressing cyber risk. We expected stronger urging to "show me the money," but that was not top priority.

*KRI: key risk indicator

[2] Wondering who Jack Jones is and what he says should/shouldn't be done? You can start here. But one of the no-no's is performing math on categorical ratings like Medium x High = 65, which is surprisingly common.

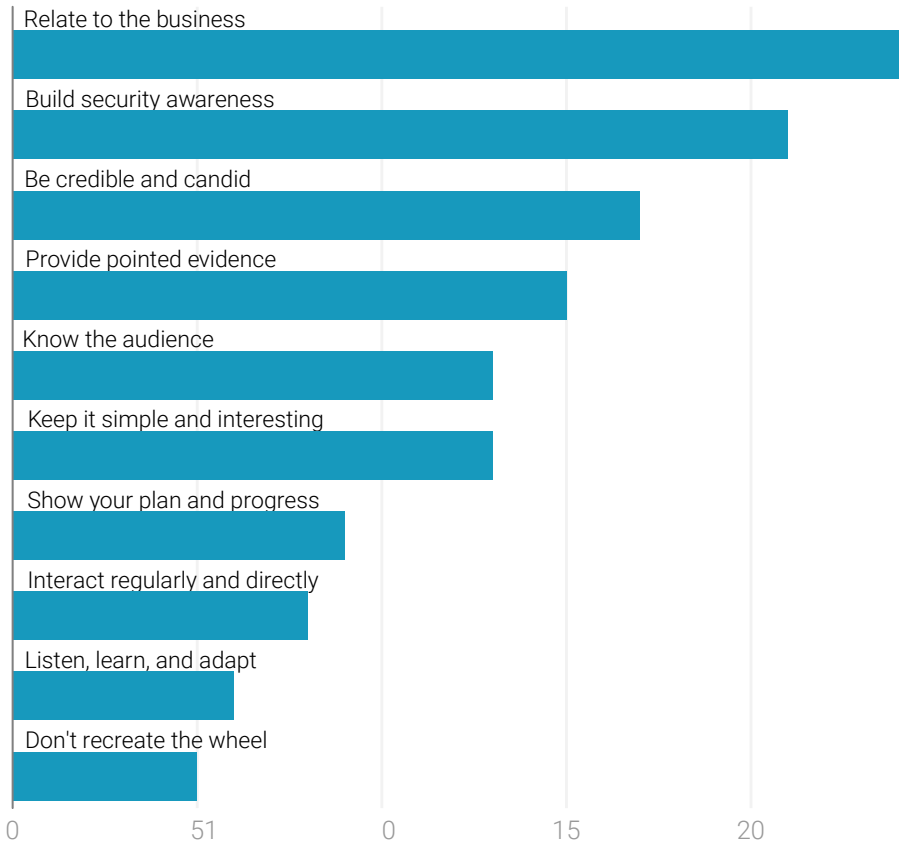
[3] The Cyentia Institute recommends *Measuring and Managing Information Risk* by Jack Freund and Jack Jones and *How to Measure Anything in Cybersecurity Risk* by Douglass Hubbard and Richard Seiersen.

BALANCE POINT 6

COMMUNICATING WITH THE BOARD

Assume for a moment that the security program is operating efficiently and doing everything it should be doing to effectively protect the business. This has been verified through appropriate metrics and credible third-party review, and all relevant information regarding risk posture and prescribed treatments is in good order. One might think the CISO's success is assured at this point, and s/he is destined to be lauded by the Board and peers as a hero to all. But not so! If all of this cannot be effectively communicated to the Board, defeat can still be snatched from the jaws of victory.

Figure 10
Tips from CISOs and Board members for communicating with the Board



Many CISOs consider interacting with the Board to be the toughest part of their job. With the hope of easing that burden, we asked both CISOs and Board members their thoughts on what would improve communication between the two parties. Their top ten tips round out this section.

BOARD PERSPECTIVE

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

Figure 10

The cybersecurity program might run on bits and bytes, but Directors want none of that in the Boardroom. Notice how soft rather than hard skills dominate the list of tips from CISOs and Board members in this figure.

BOARD PERSPECTIVE

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

1. **Relate to the business.** Information presented should be relevant to the business and understandable by the Board. Avoid security jargon.
2. **Build security awareness.** Explain key concepts and questions like "Who would target us and why would they want our data?" Use current events to make it real but avoid hype.
3. **Be credible and candid.** Project competence, honesty, humility, and openness. Share good and bad news and be clear what you know and don't know.
4. **Provide pointed evidence.** Share metrics to make a point. Talk in dollars if possible. Don't drown the Board in a sea of unnecessary details (but be ready to provide them if asked).
5. **Know the audience.** Get to know the background and expectations of the Board. Review and get feedback on what they've seen in the past.
6. **Keep it simple and interesting.** Tell a story that is easy to follow. Less is more; focus on a few topics at a time. Use analogies to connect with them.
7. **Show your plan and progress.** Create a master plan and tie everything back to it often. Inform them of goals, strategies, roadblocks, solutions, and status.
8. **Interact regularly and directly.** Communicate outside of the Boardroom. Set up one-to-one sessions if possible. Try to deal directly with the Board to ensure the message isn't lost or altered in the middle.
9. **Listen, learn, and adapt.** As you speak, teach, and prepare, don't forget to listen to the Board, learn their needs, and adapt your presentation approach.
10. **Don't recreate the wheel.** Use a recognized reporting framework. Don't fall to the temptation to redo everything right away. Talk to peers to see what's working for them.

FINDING THE BALANCE

Board members desiring to improve their own readiness to communicate with CISOs have a growing set of sources to leverage. The Cyber-Risk Oversight Handbook from the NACD is an excellent place to start and contains questions Board members can ask CISOs on various subjects.

CISO PERSPECTIVE

"Lots of people say you have to dumb it down; that's a mistake. These [Board members] are smart people. They do speak a different language, but they're not in another world and we need to build a bridge."

BOARD PERSPECTIVE

"Use two ears vs. one mouth. As much as you know infosec, they know the business. Your job is not telling them what to do but helping them with what they want to do."

CISO PERSPECTIVE

"The Board wants to hear a story. They want to know we're doing the right things to address risk, we're on par or better than our peers, and we have the resources we need without overspending."

CYBER BALANCE SHEET

What is a Cyber Balance Sheet?

A statement of the cyber assets, liabilities, and capabilities of a business or organization at a particular point in time. A Cyber Balance Sheet is used to facilitate discussions between a Board of Directors and the CISO, keeping both parties literally and figuratively on the same page.

Assets and Liabilities

Put simply, assets include anything owned by the company that has value, including the capabilities and controls the company has developed to protect its assets.

On a traditional balance sheet, liabilities include everything owed by the company. On a Cyber Balance Sheet, the liabilities column shifts to convey emerging threats, inadequacies in protection, risk exposure, current/future initiatives, etc. In fact, your assets can often become liabilities if they are not managed properly. In the same way, liabilities can flip to assets with the right strategy.

How to Use a Cyber Balance Sheet

The Cyber Balance Sheet is by its very nature an analogy to a dollars-and-cents concept that Corporate Directors understand. If you're not ready to quantify cyber risk in dollar terms yet, devise a crawl-walk-run plan to begin moving toward a shared language with your Board.

Crawling begins with all parties being concise, speaking in plain language, and working from the same starting point. Walking begins with the acknowledgment that all risks must be balanced within one of three positions:

- *Acceptance* – There will always be some degree of risk acceptance. CISOs should communicate risk acceptance using business terms and examples and assign value (quantitative or qualitative) to positive and negative impacts of risk taking.
- *Mitigation* – Risk mitigation is perhaps the largest portion of budget allocation for the CISO. As discussed in Balance Point 2, the conundrum of "proving a negative" remains a constant struggle for security leaders to justify security spending. Justify risk mitigation investments by focusing on likelihood and risk exposure. Commonsense analogies can help tell a compelling story.
- *Transfer* – Some amount of cyber risk can be transferred through instruments such as cyber liability insurance or legal language in vendor agreements. Just as with mitigation, risk transfer may still expose your organization to risks such as brand/reputation damage.

It's important to remember that Corporate Directors view value and impact to the organization through the lens of materiality. A material weakness presented to the Board must be corrected. If the Board fails to do so, it would be neglecting its fiduciary responsibility. Understanding your organization's threshold of materiality is critical for relating cyber risk posture to Corporate Directors.

Finding the balance among Acceptance, Mitigation, and Transfer ensures you are presenting a complete picture of your risk posture, enabling better awareness and more informed decisions.

Running is where we need your help. The pages that follow represent a sample Cyber Balance Sheet — one that certainly does not represent an exhaustive or definitive list of potential cyber assets and liabilities. It is, however, a place to start.

Quantifying cyber risk requires a level of shared language and risk principles that no one firm or one study can offer. As such, we humbly ask you to review the following sample Cyber Balance Sheet, and help us build a common framework over the next year from which we can all work.

ASSETS

Fixed Assets

Fixed cyber assets include the hardware that your organization depends on for normal operations — things like servers, laptops, and network devices. All are susceptible to crippling cyber attacks in the form of malware or ransomware, or devastating physical disruptions like natural disasters, theft, or misuse.

RISK POSTURE	STATUS
Acceptance	
Mitigation	
Transfer	
Materiality Statement:	

Data Assets

Data assets are some of the most valuable assets owned by a company. Data assets can be as far reaching as email data, customer data, credit card data, or medical records – but increasingly, companies are turning their attention to a subset of data, known as their "crown jewels." Crown jewels data has the most value to an organization, or the greatest potential liability if it were lost, leaked, or stolen. Crown jewels data often includes critical intellectual property, proprietary software, financial information, and executive emails.

RISK POSTURE	STATUS
Acceptance	
Mitigation	
Transfer	
Materiality Statement:	

Systems

The technology to support critical business processes represents a significant investment of capital for most companies. Security-monitoring tools, identity and access management platforms, GRC and compliance tools, and internal and external websites should all be presented to the Board as strategic assets that require protection, investment, and planning.

RISK POSTURE	STATUS
Acceptance	
Mitigation	
Transfer	
Materiality Statement:	

LIABILITIES

Fixed Assets

Failure to properly mitigate the risk to fixed cyber assets could pose a liability for your organization. Virtually all organizations must face the very real prospect of interruptions to business operations as a result of malicious software, but certain industries (like healthcare) are targeted more often.

RISK POSTURE	STATUS
Acceptance	
Mitigation	
Transfer	
Materiality Statement:	

Data Assets

Perhaps more than any other asset category, data assets are among those that keep Boards awake at night. Data presents significant liabilities for companies, including the potential for fines, penalties, and litigation following a breach; downstream damage to brand and consumer goodwill; derailment of M&A activity; and loss of shareholder confidence – all of which could result in tremendous financial losses for a company.

RISK POSTURE	STATUS
Acceptance	
Mitigation	
Transfer	
Materiality Statement:	

Systems

Systems that are homegrown, outdated, insufficient, or are not regularly receiving security patches and updates pose risk to the organization. By not operating effectively, they open the door to data loss and undetected breaches, or simply fail to serve as effective IT controls.

RISK POSTURE	STATUS
Acceptance	
Mitigation	
Transfer	
Materiality Statement:	

ASSETS

Human Capital

Salaries for IT and security workers have skyrocketed in recent years, as demand for qualified professionals far outpaces supply. Keeping a fully staffed security operations team is often one of the greatest challenges facing an organization. These resources – from the CISO to the IT help desk – should be valued as an important cyber asset.

RISK POSTURE	STATUS
Acceptance	
Mitigation	
Transfer	
Materiality Statement:	

Intangible Assets

The hardest assets to quantify, and some of the hardest to protect, are brand and reputation. Despite the difficult nature of quantifying its value, a well-respected brand is often a company's single most valuable and vulnerable asset.

RISK POSTURE	STATUS
Acceptance	
Mitigation	
Transfer	
Materiality Statement:	

LIABILITIES

Human Capital

Your employees can present significant liabilities to your organization, and on several distinct fronts. Under-trained or understaffed security and IT teams can put you at risk for data loss or business disruption. Non-IT resources are often the indirect sources of breaches, as HR, accounting, sales, and other business functions can be susceptible to external attacks.

RISK POSTURE	STATUS
Acceptance	
Mitigation	
Transfer	
Materiality Statement:	

Intangible Assets

A brand that has been tarnished by a high-profile data breach, particularly a breach that results in intense media scrutiny or airing of "dirty laundry," can quickly become a liability – as a loss of consumer or shareholder confidence can result in diminished sales and plummeting stock prices.

RISK POSTURE	STATUS
Acceptance	
Mitigation	
Transfer	
Materiality Statement:	

JOIN THE CONVERSATION

Discuss cyber risk news, trends, and ideas with other executives and Board members in our Cyber Risk and the Boardroom group on LinkedIn.

Request to join

If you are interested in contributing to the 2018 Cyber Balance Sheet Summit or Report, please shoot us an email.

contribute@cyberbalancesheet.com

APPENDIX A

KEY CONTRIBUTORS

Focal Point and the Cyentia Institute wish to thank all those who contributed their time, insights, and assistance to this research. CISOs and Board members who participated did so with the understanding that neither they nor their organizations would be publicly identified (and even private interview notes were de-identified). Some contributors represented themselves as SMEs and/or firms that provide cybersecurity services, and were kind enough to share general observations across their customer base. We would like to recognize their efforts and list those who gave permission to do so below.

Rob Arnold
Co-Founder and CEO
Threat Sketch

Anton Chuvakin
Industry Analyst

Bruce Eatroff
Founding Partner
Halyard Capital

Jean-Christophe Gaillard
Managing Director
Corix Partners

Ron Gula
President
Gula Tech Adventures

Jack Jones
Co-Founder, RiskLens
Chairman, FAIR Institute

John Madelin
CEO
Reliance acsn

Christopher Messina
Private Investor and Board Member

David Russell
Chief Engineer
Alasdair Security

Michael Scheidell
CSO and Managing Director
Security Privateers

Ed Snodgrass
Principal and CISO
Secure Digital Solutions

A special thank you to those who presented on key cyber risk and Board-level issues at the 2017 Cyber Balance Sheet Summit and to the Nasdaq Marketsite for hosting the Summit. We appreciate all Summit attendees taking time out of their busy schedules to participate in the discussion on cyber risk. Focal Point and Cyentia would also like to thank the NACD and the Internet Security Alliance and its CEO Larry Clinton for generously supplying all attendees at the Summit with a copy of the NACD Cyber-Risk Oversight Handbook. These contributions were instrumental in starting the conversation around cyber risk in the Boardroom.

John Becker
Former Chairman & CEO
Sourcefire

Yong-Gon Chon
CEO
Focal Point Data Risk

Bruce Eatroff
Founding Partner
Halyard Capital

Tracy Grella
Global Head of Cyber
AIG

Larry Handen
Senior Managing Director
Macquarie Capital

Ronald D. Lee
Partner
Arnold & Porter Kaye Scholer

Christopher Messina
Private Investor
Board Member

Tom Reagan
Managing Director, Cyber Practice Leader
Marsh & McLennan

Joel A. Schleicher
Chairman of the Board
Focal Point Data Risk

Kiersten Todt
Former Executive Director
Presidential Commission on
Enhancing National Security

APPENDIX B

GLOSSARY

The descriptions below correspond to the figures presented in this report and are included to aid in proper interpretation.

Balance Point 1 | Figure 1

Security guidance:
Drive awareness, provide guidance, build knowledge, etc.

Business enabler:
Build secure products, support sales, enable revenue, etc.

Loss avoidance:
Reduce losses, lower risk, preserve revenue, etc.

Data protection:
Prevent data breaches and disruptions

Brand protection:
Avoid harm to the corporate brand and reputation

Balance Point 2 | Figure 3

Board awareness:
The Board's level of security awareness, knowledge, etc.

Presentation skills:
What and how security information is presented to the Board

Business enabler:
Extent to which the Board views security as a business enabler

Board support:
Level of interest, support, budget, etc. the Board gives to security

Offer justification:
The ability (or lack thereof) to justify security decisions and directions

Conservative spend:
A conservative approach to needs, budgets, and expectations

Prior breach:
The company had a recent breach that affected Board perception

Balance Point 3 | Figure 5

External standard:
Security standards and frameworks like NIST CSF, PCI-DSS, CIS Controls, etc.

Risk assessment:
Loose definition used here; assessment of frequency, impact, criticality, etc.

Maturity model:
Evaluation of the maturity of various security-related capabilities

Audit (external & internal):
External and internal audit of the security program and controls

Custom program:
An internally designed security program not based on external standards

***Ad-hoc* approach:**
No formal assessment method; just doing what's needed as needed

Diagnostics/KPIs:
Regular diagnostics or indicators used to assess security status

Peer benchmarks:
Comparative metrics and scores within peer or industry groups

Balance Point 4 | Figure 6

Assets and users:
Devices, data, users, accounts, etc. under management

Awareness activities:
Staff training records, security awareness campaigns, phishing tests, etc.

Governance info:
Updates on security planning, spending, staffing, projects, etc.

System vulnerabilities:
Critical vulnerabilities, patching levels, penetration test findings, etc.

Incidents/events:
Attacks, incidents, infections, breaches, violations, abuse, etc.

Response metrics:
False positives, time to detect/remediate, ops tickets open/closed, etc.

Compliance/maturity:
Implementation and maturity of security controls and standards

Peer benchmarks:
Comparisons of security posture and KPIs to peer organizations

Risk posture:
Assessment of organizational exposure to various IT-related threats

Business enablement:
Revenue, sales, interactions, etc. supported by the security program

Balance Point 5 | Figure 8

Descriptive:
Purely qualitative description of risk and/or risk factors (threats, vulnerabilities, etc.)

Control deficiency:
Risk assessment based solely on control implementation or quality

Categorical:
Rating of risk according to categories like high-medium-low

Numerical score:
Deriving a risk score through some operation (e.g., likelihood(2)*severity(5)=10)

Expected losses:
An estimate of total losses expected within a given timeframe

Impact estimate:
Risk assessment based solely on potential (often worst-case) impact

CYBER BALANCE SHEET

BOARD PERSPECTIVE

"ULTIMATELY, SECURITY EXISTS TO INCREASE SHAREHOLDER VALUE."