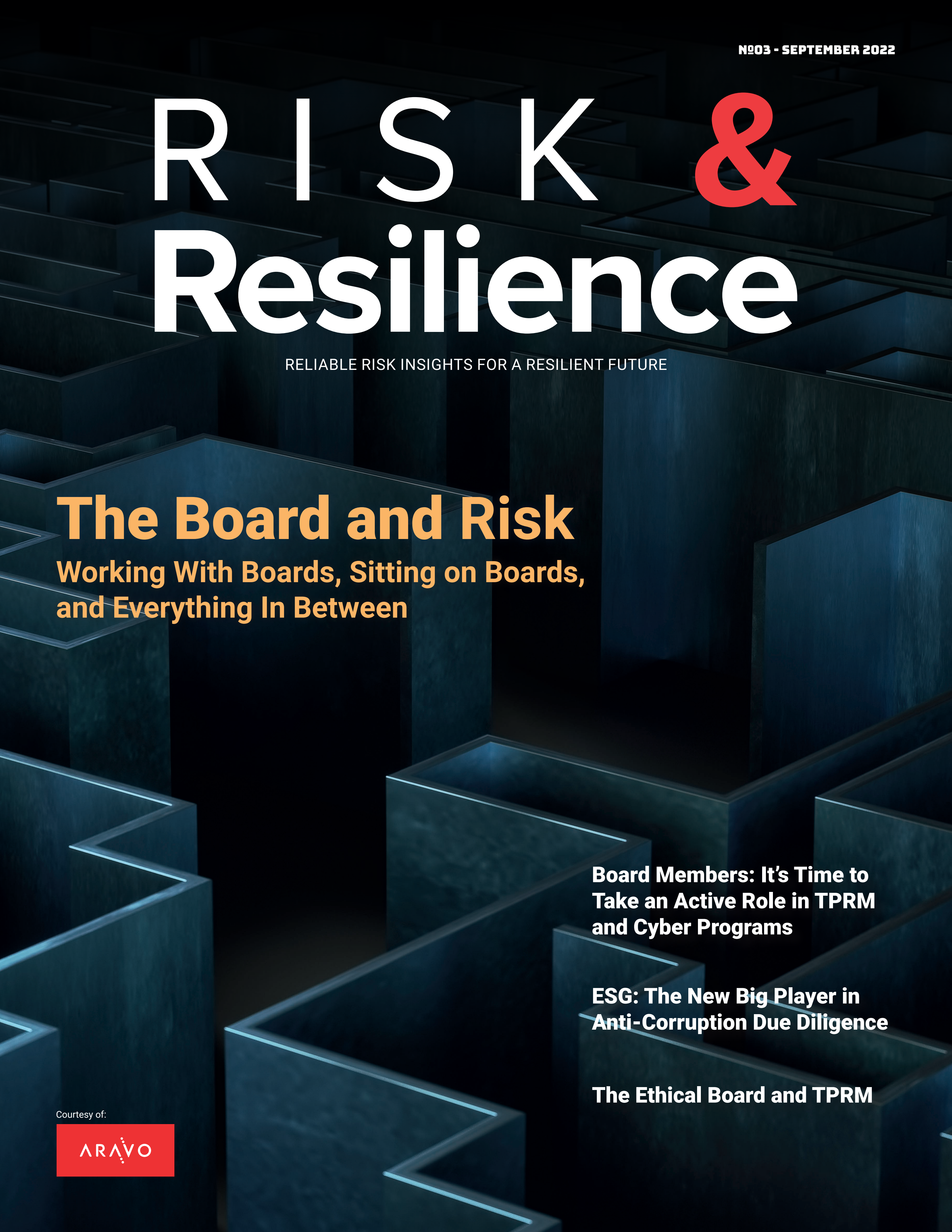


№03 - SEPTEMBER 2022

RISK & Resilience

RELIABLE RISK INSIGHTS FOR A RESILIENT FUTURE

The Board and Risk

Working With Boards, Sitting on Boards, and Everything In Between

Board Members: It's Time to Take an Active Role in TPRM and Cyber Programs

ESG: The New Big Player in Anti-Corruption Due Diligence

The Ethical Board and TPRM

Courtesy of:
ARAVO

RISK & Resilience

Editor in Chief
Hannah Tichansky

Production & Advertising Manager
Rebecca Waltz

Contributors
Barbara-Ann Boehler
Matt Kelly
Colin Campbell

Creative Director
Cindy Rucker

riskandresilience.co

LinkedIn: risk-&-resilience-magazine

Be a Part of R&R:
Interested in being featured in the next issue of Risk & Resilience?

We are always looking for experts, thought leaders, and practitioners to participate in interviews and articles.

Email info@riskandresilience.co to let us know.

No part of this publication may be copied, reproduced, transmitted or held in a retrievable system without the written permission of the publisher Aravo Solutions, Inc. While every effort is made to ensure the accuracy of all material published in Risk & Resilience, the publisher accepts no responsibility for any errors or omissions, nor for any claims made as a result of such errors or omissions. Views expressed by contributors are not necessarily those of the publisher. Any statements expressed by professionals in this publication are understood to be general opinions and should not be relied upon as legal or financial advice. Opinions expressed herein do not necessarily represent the views of the author/interviewee's firms or clients.

Risk & Resilience reserves the full rights of international use of all published materials. Risk & Resilience retains the right to reprint any and all editorial material for promotional use, with credit given.

SUMMARY

4 Demonstrating Good Governance: Communication and the Board of Directors

6 ESG: The New Big Player in Anti-Corruption Due Diligence

9 Gaining Clarity: TPRM & the Board

13 An Evolving Cybersecurity Risk Management Landscape

16 How Board Members Can Build A Mental Resilience Toolkit for Their Organization

20 TPRM & Boards: Regulatory Change is Coming

24 The Ethical Board and TPRM

28 With New ESG and DEI Rules Comes Additional Complexity - and Opportunity - for Board Directors

32 Board Members: It's Time to Take an Active Role in TPRM and Cyber Programs

36 Enhanced Board Reporting on Supply Chain Risk is Essential

INTRO

Demonstrating Good Governance

Communication and the Board of Directors

With great power comes great responsibility. This is true for superheroes and members of corporate boards alike. It is well known that board members are charged with ensuring good governance by shaping corporate policy and making fiscally responsible decisions. However, with the attention of ESG concerns, the Board is also tasked with helping to ensure that the corporation (and its partners) proceed ethically. The Board answers to its shareholders, but it also must answer to its consumers and even the general public. Social networks have provided connectivity, transparency, and the speed of communication to a higher degree than any other time in history.

This means that the decisions made by boards of directors are going to be examined by the public, and the public has had a tough couple of years. The appetite for corporate mismanagement is low. Optics are incredibly important. A few months ago, much was made in the news about the corporations who remained invested in Russia. The public outcry for divestment trumped any financial goals of the corporation. In this culture of private messages going viral, Yelp reviews, TikTok videos, and Twitter rants, corporations will be held accountable if they act in a way or further the bad actions of other entities against the public's opinion. The headlines are riddled with examples and case studies of not only purposefully fraudulent corporate malfeasance, but also just plain old inattention to detail and fundamental breakdown in communication.

In our newest issue of Risk & Resilience Magazine, we examine the role of the Board of Directors. We interview those who serve in the role as well as those who report to, work with, and support the role. Throughout all of our conversations and research in the area there was one theme in particular that clearly and unequivocally emerged. This theme is not shocking, it's not based on new data analytics or cutting-edge technology, it's not driven by enhancements in software, AI, machine learning, or quantum mathematics. It is both incredibly simple to fathom and unfathomably difficult to implement. The most important aspect of working on, with, and for the board, is communication.

"The most important aspect of working on, with, and for the board, is communication."

> “Board reporting is not a tick-the-box exercise, it is an opportunity for senior leaders to ensure that they are educating their Board of Directors on the issues at the firm.”

Good communication is certainly a requirement in nearly every endeavor imaginable. However, good communication between the business and the Board of Directors is an imperative and a hallmark of good governance. Board members must understand what is happening throughout the corporation in order to make informed, reasoned, and sound decisions.

Board reporting is not a tick-the-box exercise, it is an opportunity for senior leaders to ensure that they are educating their Board of Directors on the issues at the firm. In Aravo’s most recent survey, “Gaining Clarity,” we noted that comprehensive investment in a third-party risk management platform resulted in a mature program and in less of an impact on incidents reported. Note that a solid program results in less incidents. This is how we know that the program is working. However, we also know that mature programs are resilient programs. The only way to obtain the level of investment necessary is to have a Board of Directors that is educated on risk, and the ability to effectively communicate the value of the program to the Board.

We hope that you find this issue of Risk & Resilience helpful whether you are a board member, considering board membership, or regularly report to a board.

ESG: The New Big Player in Anti-Corruption Due Diligence

Insights from a Board Advisor

Andrew Henderson
Senior Advisor at Speeki

Risk & Resilience Magazine sat down with Andrew Henderson, Senior Advisor at Speeki. Speeki is an ESG, compliance, and whistleblowing platform, helping companies improve their brand experience, earn a better reputation, and manage risk by enhancing their awareness and management of ESG. For this interview we discussed his experience as an advisor to boards, and what should be on boards' radars in the year ahead.

Could you describe your experience working as an advisor to boards of directors?

I've done a lot of work helping both chief compliance officers and their boards understand the need for compliance. Originally, that was surrounding anti-corruption compliance and getting the board to understand the benefits and why it's not just a cost. So, a lot of it was training- helping them understand the value of compliance and the value of being able to control their business in that way.

Have you historically been focused on boards in a particular industry? Primarily financial services or are these boards cross-industry?

Certainly, financial services, but also very much healthcare, mining, and extractive heavy industries. Basically, companies with a large global footprint on the sales and supplier channels. More recently I've worked in the corporate space, which is a lot more work, mainly because of ESG as well as the fast-moving consumer goods industry which wasn't previously a big player for anti-corruption due diligence. But now they're very much at the forefront of ESG discussions.

What are you seeing as some of the top legal, regulatory, or compliance challenges that are facing boards currently?

The broad topic of the day is ESG- at the moment it's quite early stages for a lot of boards. They don't always really understand what it is, they just know they have to be involved in it somehow, but they don't generally have clear plans as to what they need to do. I think the difference between ESG from the anti-corruption work that we were doing previously is that the driver for it is actually more external than internal. Boards are being asked by their investors and especially on the financial side, the shareholders are asking what they're doing around ESG. The ratings agencies are rating them according to their ESG output, what they're publishing, as well as the indices.

But it doesn't mean it's any easier for a board to have a clear policy and view

“ESG is such a nebulous topic. It means a lot of different things to a lot of different people... But there’s a lot more in there in which customers and their boards or senior management need to work out what they want to do.”

on what they need to do. Mainly, this is because ESG is such a nebulous topic. It means a lot of different things to a lot of different people. I think most of the focus of ESG at the moment is very much around environmental, carbon emissions, et cetera, and a little bit on the human rights angle. But there’s a lot more in there in which customers and their boards or senior management need to work out what they want to do.

As an advisor, how can boards get started on boosting their resilience and reducing ESG risk within their organizations?

Certainly, in the work that I’ve done, we’ve always tried to use some of the ISO standards, like 19600, and some of the other frameworks, or the federal sentencing guidelines. It’s important to think about what are the risks that you’re really trying to address? What are the resources you’re going to put into that? How are you going to do training, how do you report up to the boards? It’s a very similar process with any other compliance program. I suppose again, the only difference with the ESG world is the reporting is not just to a board, but reporting to a board and then reporting out from the company to its investors and stakeholders.

How important are you finding technology in supporting compliance?

I think it's absolutely vital. For good or bad, I suppose. I think 10 or 20 years ago, people would not have been asked to look down their supply chain for any of these risk areas. They're just so vast, that you couldn't put 20,000 or a hundred thousand supply chain elements into any sort of older system that could give you any viable information. But now there are plenty of providers to support the volumes of suppliers that people are trying to deal with… Now that the technology is there, people are expected to actually look at the data they already hold.

Are there specific issues or types of risks that boards should be paying attention to? Maybe things that are not yet on their radars?

Most of the risks are on radars at some level. I think it's the assessment of which ones are most critical that's important. I think people tend to focus on the last issue that they heard about, certainly things like cybersecurity. It has to be on the top of everyone's agenda because of the impact it has on the business… So, it is the kind of risk that goes straight up to a board that people need to really think about. Whereas a lot of the other risks are not going to stop the company from operating. So, I think those kinds of risks have to be seen at the right level and have to be resourced properly to manage them.

And I think the ESG topic will continue to grow. I think it's really the ability for companies to show, to some extent, their ethical or moral standing, and let investors make their choices based on that rather than just being a pure financial discussion. We're still in the early days of that. And I think it's a little binary to say, you're good at ESG or you're bad at ESG. But eventually, we'll work it out in a way that people can actually judge the kind of risks and the nuances in a way that they can make assessments before they're making investment decisions. Which will be a great step forward. But we've got a little way to go before we're there.

This interview has been edited for length and clarity.

About the Contributor:

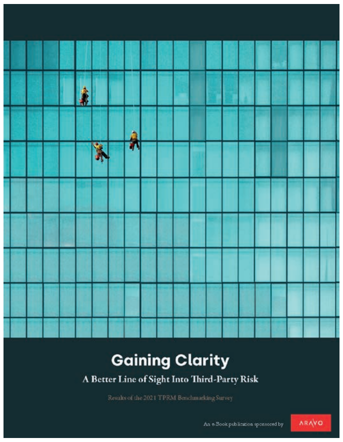
Andrew Henderson is a Senior Advisor at Speeki. In his previous roles, Andrew has assessed, designed, implemented and managed compliance programmes for multinational organizations across a wide range of industries. He has been involved in the design and development of data products, services, and workflow platforms, and retains a key interest in using technology to support compliance. Andrew has degrees in Law and Information Technology.

> "I think it's a little binary to say, you're good at ESG or you're bad at ESG. But eventually, we'll work it out in a way that people can actually judge the kind of risks and the nuances in a way that they can make assessments before they're making investment decisions."

SURVEY

Gaining Clarity: TPRM & The Board

Results of Aravo's 2021 TPRM Benchmarking Survey



Gaining Clarity

A Better Line of Sight Into Third-Party Risk

Results of the 2021 TPRM Benchmarking Survey

An e-Book publication sponsored by ARAVO

In its fourth annual TPRM benchmarking survey, Aravo interviewed over 100 risk and compliance professionals to analyze TPRM trends providing important data points that will help firms benchmark their programs. A key portion of the survey examined the role of Boards into their TPRM programs, board oversight activities, and its relation to program success. This article originally appeared in the benchmarking survey.

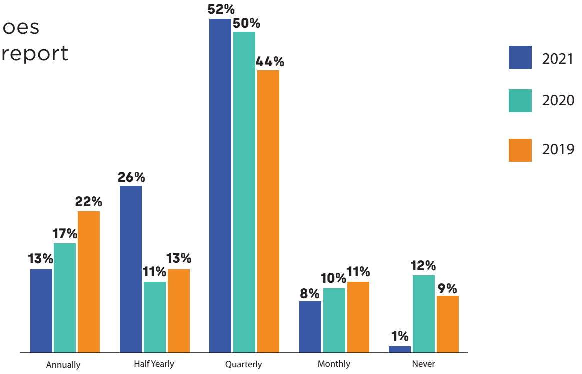
Given good, actionable information, it's likely that boards will understand third-party risks more deeply. Boards also hold the power to ask the right questions of management about third-party risk and to ensure it has the right attention and resource in the organization.

A quarterly cadence of board reporting remains normal

52% of respondents who knew how often their organization reported to the board indicated that this reporting took place quarterly, which is only slightly changed from 2020 when it was 50%. The number of organizations reporting annually fell from 17% to 13%, while the number of organizations reporting half yearly nearly doubled from 11% to 26%. About 8% report monthly, compared to 10% last year.

The number of respondents who never report to the board dropped significantly, from 12% in 2020 to only 1% in 2021. The number of people who indicated that they didn't know also dropped significantly. In 2020, 14% of respondents didn't know if their TPRM organization was reporting to the board. In this survey, that number is only 1%.

Chart 1: How often does your TPRM program report to the board?



Cybersecurity continues to be the largest concern for boards, but efficiency and cost-cutting are a growing issue

As in previous years, cybersecurity is decidedly the most important concern for boards at 26%. Historically, reputational risk has been the second-highest, but in this survey, it fell into the lower half of responses at just 9%. The second-greatest concern is now cost-cutting and efficiency, which has leapt to 17% in 2021, compared to just 5% in 2020. It is followed by compliance risk at 13%.

Operational risk, personal liability, and financial risk all came in at 10%. It's interesting to note here that concern related to personal liability, which at 1% was the least reported concern in previous surveys, significantly increased in 2021. Business continuity (a new category added in the 2021 survey) was the greatest concern for about 3% of boards and strategic risk was the lowest at just 2%. Answers in the "other" category included concern that "Vendor Risk Management does not exceed the Risk Appetite Statement parameters for all risks" and "a combination of Reputation, Compliance, and Financial Risk."

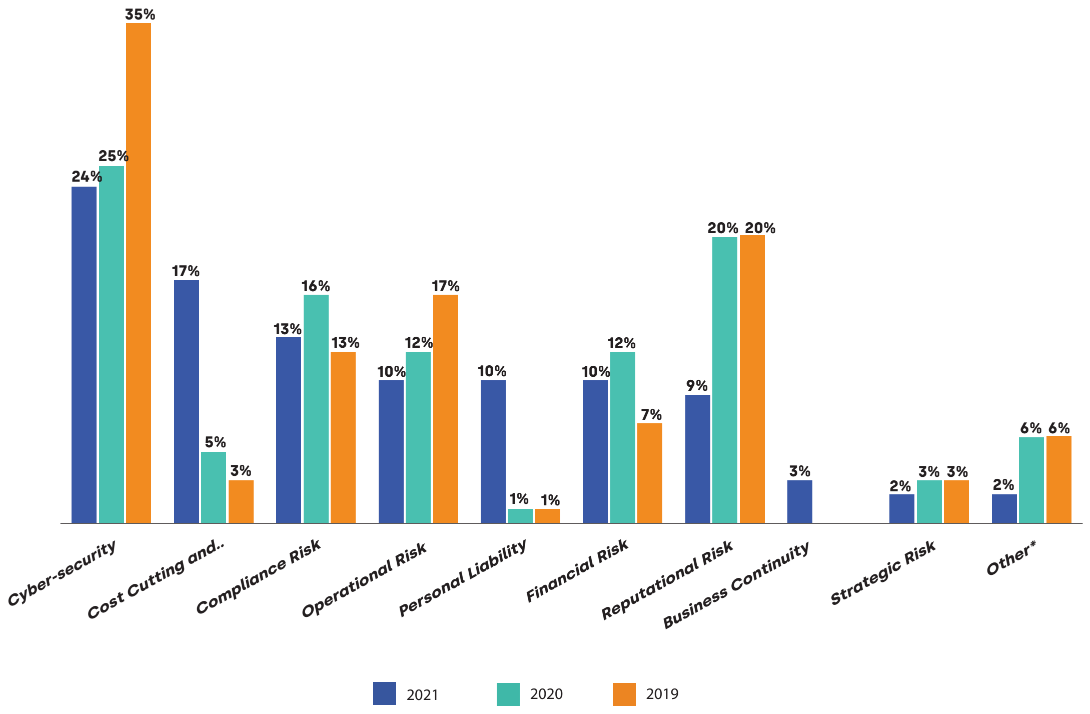


Chart 2: Top TPRM-related concerns of boards by year

Board engagement is increasing as respondents report more boards are exercising a moderate or high level of oversight

In 2020, more than 1/3 of respondents (34%) indicated that their board had only a low level of oversight. This year, the percentage of respondents who indicated their board had only a low level of oversight fell by almost 2/3 to 13%. The biggest gain was amongst boards that demonstrate a moderate level of oversight (69%). Those who said their boards showed a high level of oversight rose to 18% in 2021.

This shift was not unexpected. For many, the events of the previous 18 months underscored the reliance on third parties and the potential for disruption. Boards appear to be stepping up to minimize impacts to the business, and the role of TPRM in the organization likely has greater exposure as it becomes a key priority.

And it appears that practitioners have greater insight into the board's level of engagement. Only 5% of respondents didn't know how engaged their boards actually were. In 2020, 13% were unaware of the board's level of engagement.

How would you categorize board engagement with your third-party program?

	2021	2020	2019
High level of oversight – the board drive it and are actively engaged in reviews and alignment to corporate strategy.	18%	15%	21%
Moderate level of oversight – our board are aware of it, they are notified of critical incidents, and they provide some governance.	69%	51%	52%
Low level of oversight – Third-party risk management is not a key priority for our board.	13%	34%	27%

Table 1: How would you categorize board engagement with your TPRM program?

Boards have a better handle on the third-party risks their organizations are facing

The increasing engagement is likely the reason for a corresponding increase in confidence of TPRM practitioners regarding the board's ability to understand and navigate this environment of increased business risks. A total of 88% of respondents feel their board has a good handle on the third-party risks the organization is exposed to.

Generally speaking, do you think your board has a good handle on the third-party risks your organization is exposed to?

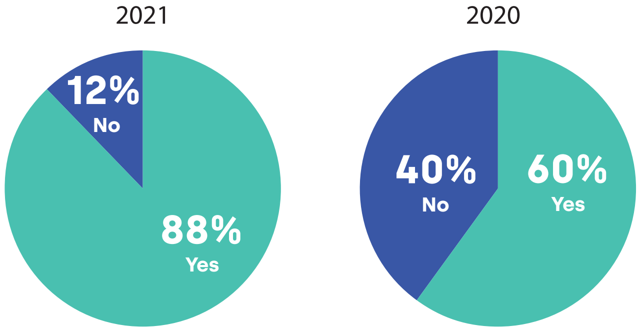


Chart 3: Do you think your board has a good handle on the third-party risks your organization is exposed to?

An engaged board is more likely to result in mature programs

Like any initiative, TPRM typically needs sponsorship at the board and senior management levels, which was clear in this year's survey. Only respondents with high levels of board engagement indicated that they had agile programs.

While about 17% of programs with high board engagement were classified as Agile, a surprisingly high number (39%) were at the Ad Hoc stage. This is significantly higher than the 8% of organizations that reported a high level of engagement and being at the Ad Hoc stage. The increase in board engagement compared to previous years may not have translated into broad program initiatives yet.

These programs may also be newer ones initiated by board involvement that haven't had time to mature yet. However, 61% of organizations with low board engagement report that their programs are low maturity (Ad Hoc or Fragmented). About 51% of organizations with moderate board engagement reported low maturity.

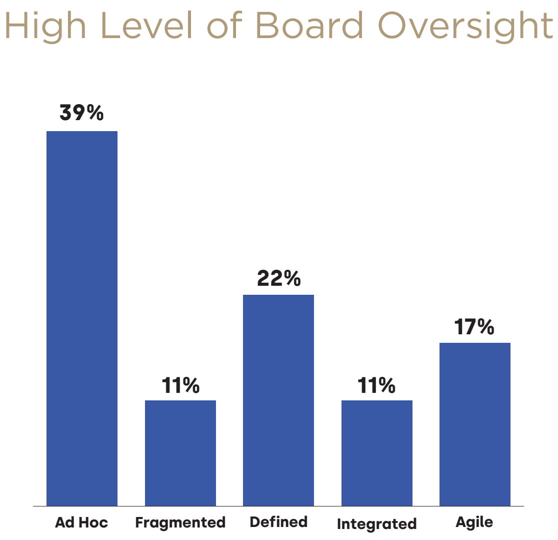


Chart 4: Maturity of Programs reporting high board engagement

Boards hold an important oversight function in third-party risk management. They need to understand their duty of care and ensure actions taken at the board meetings are properly documented to provide evidence that directors exercised their fiduciary duties, as seen in other articles included in this edition of *Risk & Resilience Magazine*.

If you are interested in additional TPRM benchmarking insights we invite you to explore the full survey.

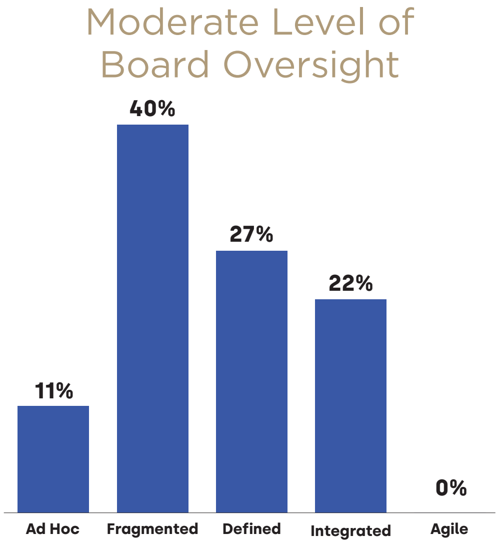


Chart 5: Maturity of Programs reporting moderate board engagement

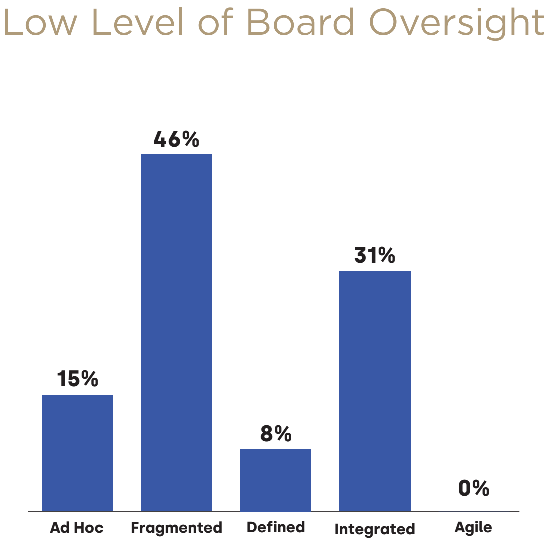


Chart 6: Maturity of Programs reporting low board engagement

EXPERT CONTRIBUTOR

An Evolving Cybersecurity Risk Management Landscape

The Rise of CISOs as Boards' First Line of Defense

Matt Kelly
Editor and Founder of
Radical Compliance

RADICAL COMPLIANCE
SHARP THINKING ABOUT COMPLIANCE, AUDIT, AND RISK

Corporate boards are always quick to say they worry about cybersecurity, but a question lurks behind that statement that few people take the time to consider fully.

What does "worry about cybersecurity" actually mean?

After all, boards could worry about the regulatory enforcement that comes from poor protection of personal data; or the operational threats that come from a ransomware attack; or the strategic weakness of being unable to demonstrate your cybersecurity to potential customers.

The truth, of course, is that boards **try** to worry about all three issues, plus the many other ways that cybersecurity can flummox an organization; they just don't know how to approach all these issues in an effective, disciplined way. Or, to phrase the governance issue here more formally: boards struggle to set business objectives and tailor corporate strategy in a way that respects the cybersecurity risks their organizations face.

That struggle is an opportunity for the CISO — if you can seize it.

Why Are Boards Overwhelmed?

That's easy. Modern technology has allowed organizations to bring one business process after another into the digital era. The financial and efficiency gains from that digital transformation are enormous, but digital transformation also **changes what cybersecurity is about**. Today, cybersecurity is every bit as much about strategy and governance, as it is (and always has been) about regulatory compliance and documentation.

For example, once upon a time, most boards' top cybersecurity concern was privacy compliance. Directors wanted assurance that personal information was secure and that the company could notify regulators and consumers promptly when a breach happened — but those were tactical steps a company would need to take only when a privacy breach happened.

Today's risks are more pervasive and entrenched at the same time. Ransomware attacks could halt operations for days on end, which might harm revenue projections or lead to civil lawsuits. Relying on cloud-based technology providers might lower some operating costs, but drives up others since attacks might come through those tech providers to harm your organization. (That's precisely what happened in the Solar Winds attack of 2020 when Russia electronically fleeced hundreds of U.S. businesses by infecting a Solar Winds software patch with malware.)

Technology has seeped into so many business operations, so deeply, that for all practical purposes cybersecurity and operational risk have fused into a single headache for the board. Directors can't ponder any change to operations without considering the IT and cybersecurity risks that are involved.

For better or worse, most boards don't yet have the expertise to navigate those issues well. They need help — and the CISO is the logical candidate to offer it.

> "The financial and efficiency gains from that digital transformation are enormous, but digital transformation also changes what cybersecurity is about. Today, cybersecurity is every bit as much about strategy and governance, as it is (and always has been) about regulatory compliance and documentation."

What the CISO Can Do Here

Foremost, the CISO can **advise** the board on the IT and cybersecurity risks that threaten business objectives.

For example, rather than simply telling boards, "Yes, we conducted the required penetration testing and compiled appropriate breach response plans." The CISO could advise the board about the merits of using third parties to provide mission-critical services. (Say, shifting to an independent contractor sales force, which might save on HR costs but could require considerable new access controls and policies.) Or the CISO could counsel the board about new compliance demands that might come from new ventures, such as bidding on government contracts, and how well the company could or couldn't implement necessary new controls.

CISOs could also help boards by developing or explaining the Key Risk Indicators and Key Performance Indicators that are more useful in today's digitally transformed world, where so much of success depends on third-party service providers meeting performance goals. Boards won't just want to know that the company is meeting its cybersecurity compliance obligations; **they will want assurance that the organization's cybersecurity risk management is strong, or a plan to bring it to proper strength**. You, the CISO, will need to figure out which metrics tell that story.

Briefing the board on specific compliance efforts will still be a part of that story; compliance issues never go away. But compliance is now only one part of the larger risk management picture the board is trying to see.

> "CISOs could also help boards by developing or explaining the Key Risk Indicators and Key Performance Indicators that are more useful in today's digitally transformed world, where so much of success depends on third-party service providers meeting performance goals."

What CISOs Need to Fill That Role

Many CISOs would welcome the chance to be a more valuable adviser to the board — but how would you do that successfully? What resources, knowledge, and relationships would you need inside the organization to deliver that higher level of insight in the boardroom?

First, you will need better ties with operating units in the First and Second lines of defense. That means better ties at a **personal** level (such as through regular meetings of an in-house risk committee) and better ties at an **informational** level (where you receive current data about each unit's IT operations and security risks).

Second, you will need insight into the organization's current state of compliance and various risk mitigation efforts that might be happening. This means you'll need a system to track compliance with various frameworks (COSO, NIST, ISO standards, and the like), where you can see at a glance which controls connect back to what requirements, and whether those controls are designed and working properly.

Spoiler alert: not all your controls will work as needed. So, a third need here is strong internal reporting and escalation procedures. CISOs need to know that when an attack or IT failure happens, the right people are alerted quickly. That includes alerts to you so that you can then (if necessary) alert the board.

Fourth, CISOs need a familiarity with breach disclosure requirements, so that they can warn the CEO or the board when an incident will need to be announced beyond the walls of the company. This doesn't necessarily mean that the CISO needs to memorize all disclosure requirements for every regulation; but at the least, you will need a mechanism to tell you, essentially, "This sort of breach has happened, which will require the following disclosures in these time frames."

That's a lot to put upon a CISO, but it can be done. You'll need technology, processes, and interpersonal skills, and also strong support from the board, to rally other senior executives and the rest of the organization to this higher level of cyber governance.

Then you can pay back that support with better insight on how to drive the business forward.

About the Author:

Matt Kelly is the founder of Radical Compliance, which provides consulting and commentary on corporate compliance, audit, governance, and risk management. Radical Compliance also serves as the personal blog for Matt Kelly, the long-time (and now former) editor of Compliance Week. Kelly writes and speaks frequently on corporate compliance, audit, and governance, and now works with various private clients to understand those fields and to develop go-to-market strategies or provide other assistance in reaching audiences of compliance professionals.

INTERVIEW

How Board Members Can Build a Mental Resilience Toolkit for Their Organization

A Conversation on the Importance of Mindfulness in the Workplace

Leonard Shen
Board Member at
OFX North America

OFX

Could you briefly introduce yourself and your career as a Financial Services Board Member?

After graduating from Harvard College and Harvard Law School in 1984, I went into environmental law and spent the next 18 years as a Justice Department trial attorney, US EPA official, US Senate chief counsel, private law firm practitioner, and in-house counsel at GE.

In 2003 I began my corporate compliance career, spending the next 17 years as global Chief Compliance Officer of GE Commercial Finance, American Express, PayPal, and Visa, including being brought in to resolve some very difficult regulatory enforcement situations. A year and a half ago I retired from Visa and joined the Board of OFX North America, part of a publicly-traded and regulated foreign exchange provider serving millions of customers worldwide.

I'm also on the Board of Silicon Valley's largest provider of shelter and services to the homeless, and teach online classes in Qi Gong, an ancient Chinese well-being practice with elements of tai chi, yoga, and meditation.

You're passionate about promoting mental resilience within the workplace. Could you explain what this is?

Mental resilience is the ability to bounce back quickly and unflappably from the inevitable slings and arrows of life… and even transmuting the stress and negative energy of an incident into a positive learning experience, coming out stronger than when you went in. Many tools can be part of the Mental Resilience toolbox. I think of them in two buckets: internal, and external. Here are my top 5 in each category.

Internal Tools:

1. **Mindfulness:** Focus on the present moment and your bodily sensations as a way to center yourself in periods of high stress. Mindfulness and meditation have been shown by a host of scientific studies to reduce reactivity, and increase levels of compassion and resilience– even changing the brain itself after just 8 weeks of moderate practice.

2. **Box Breathing:** Used by first responders, SWAT teams, and the military: inhale through your nose deep into your belly to a count of 4, hold the breath for a count of 4, exhale to a count of 4, hold out the breath for a count of 4, then inhale again etc.

3. **Take the Long View:** When something bad happens or you didn't do as well as you had hoped, don't kick yourself and wallow in it. Take the long view- will this really matter a year or five years down the road? Don't you have a track record of many other good achievements that provide context and dilute the impact of today's mistake?

4. **Take the Other's View:** If you're in a controversy with someone else, take a minute to sit in their shoes and try to internalize their perspective and why they feel that way, including assumptions about the facts which may differ from yours, and develop possible common ground with your own views and history.

5. **Exercise, Sleep, Diet:** It's so basic, yet so many of us don't do this: go outside and run around the block, go for a swim, a hike- anything to get the juices flowing and clear the mind. It will help you sleep better and process the situation and maybe help your subconscious develop a solution with the change in energy and attention. And if you improve your overall level of fitness with healthy food, exercise, sleep, etc., you will be naturally able to deal in a non-reactive way to a new stressor.

External Tools:

The external tools are general good management practices honed by the best in private industry and the military and backed by voluminous scientific studies over the years. These include:

1. **Train Creativity:** Training people to use their creativity and right brain (art, music, visual), as opposed to the analytic left brain, will increase right and left-brain connectivity and greater mental agility in times of crisis. The brain will be able to marshal more of both hemispheres and think "out of the box" when a crisis hits. This is often a critical crisis management skill, since established patterns and expectations are suddenly no longer valid, and the brain will need to quickly adjust to a new set of circumstances and assumptions. Agility is a premium trait for mental resilience.

2. **Create Safety, Reinforced Every Day:** Particularly for team leaders and managers, one of the best ways to build your staff's resilience is to show over time that it is safe for them to take risks and make mistakes, as long as they genuinely and constructively learn from them. When a track record of many genuine learnings from errors has accumulated with the continued support of their manager, employees will know when the next true crisis hits that their manager "has their back" and will support them within reason. Unburdened by fear that they will be unreasonably criticized and are trusted to perform in a time of crisis, employees will be able to focus on getting the work done, operating confidently and with a clearer head rather than in a cloud of anxiety and second-guessing.

3. **Community:** Scientific literature (and common sense) show that one of the most critical ways to ensure resilience is to have a strong support network- at work and at home. We've seen how the isolation from the pandemic lockdowns has contributed to an increase in mental illness worldwide. Managers during the pandemic have appropriately been redoubling their efforts to create team interactions and foster a familial atmosphere, particularly among workers hunched over the laptop in their homes who may otherwise be isolated from support networks.

4. **Realistic Hope:** The CEO of the company where I worked in the pits of the 2008 financial crisis used to emphasize that his role was to "Define Reality while Offering Hope." Studies have shown that giving the team the harsh realities, but also a road forward and reason to hope for better is core to preserving resilience in a crisis.

5. **Mission:** Further tying the road forward to the underlying mission or purpose of the team, the company, or the employee's own core motivators will also give people a North Star to fly toward as they toil through the worst of day-to-day stress. It's well established that when employees have a clear sense of the unit's strategy, mission, and how they fit into the big picture vision they will work harder and with greater thoughtfulness to tailor their day-to-day tasks to support the broader mission.

> **"One of the best ways to build your staff's resilience is to show over time that it is safe for them to take risks and make mistakes, as long as they genuinely and constructively learn from them."**

Why were you so drawn to Mindfulness and Resilience?

After several decades of being the classic type A, intense guy driven to excel in school and the workplace, I was encouraged by some teammates to try yoga and meditation. I found that the calming techniques and mind games from a concerted practice of mental resilience made me happier and more productive and resilient. I couple those internal techniques with best management training provided by mentors, executive coaches, and companies. They have placed a premium on building a highly engaged workforce in times of great crisis, including the 2008 financial meltdown, resolving major government enforcement actions, and threats to the brand. These have allowed me to develop and train teams with these principles.

Why should Board members prioritize mindfulness and resilience training within their organizations, when they're also dealing with things like cyber risk, supply disruptions, etc.?

I've been a firm believer that a leader's primary responsibility is to increase the skills and capabilities of their staff. You can always hire technical experts or learn about the crisis du jour. But what makes a team great, and greatly effective, is where everyone has superb EQ, relationship, and stress management skills, which they can then deploy no matter what the crisis happens to be.

These long-term, permanent capabilities will result in everyone working optimally as a team whenever the next stressor hits, with all 8 pistons hitting at the same time, rather than spinning wheels or creating internal friction that wastes everyone's energy and takes their focus away from the job.

I saw this when I was on the rowing crew in college. When all 8 oars were dipping into the water at the same time, and coming out of the water at the same time, the boat had a huge surge in forward movement – crew people call it "swing". But if even 1 oar was out of sync swing couldn't happen. There was an ineffable joy when everyone in the boat felt the swing going. You can feel that in an optimally functioning workplace, too… maybe what they call "flow" these days.

Are there additional benefits in terms of building trust throughout the extended enterprise?

There are ripple effects of even one person being mentally resilient. When that person (especially a leader) is the calm at the center of the storm, it fosters calm and efficiency in the rest of the team. We all know that – one yelling boss can instantly destroy morale and bring out insecurities and counter-productive behaviors in the rest of the team. Whereas if the people managing the crisis are calm and project confidence, everyone calms down and focuses on getting the job done.

A happier workplace of course has many benefits, whether it is attracting and retaining top talent, increasing creativity and productivity (often because people will simply work harder and better when they like where they work), or strengthening customer relationships. Customers can tell when your staff are happy and like where they're working.

Where do you see the future of mental resilience heading?

A lot of companies have been making strides, especially because of the pandemic, in building entire employee mental health programs for their staff. These help people learn the Internal skills noted above.

But with once-in-a-century challenges like the persistent and unpredictable pandemic and the most volatile geopolitical environment since World War II, I think the next several years will drive an unforgiving, increasingly Darwinian environment. This will favor not only companies who continue to deepen and broaden their mental health programs, but also those who double down on the premium management principles which foster purpose, community, reasonable risk-taking, creativity, and the other tools that underlie resilience. More than ever, they'll need to recruit, train, and reward leaders who have humane, empathetic, and supportive management styles, who will create safe spaces and model team-focused behaviors.

If a Board wanted to prioritize this, what steps could they take to get the ball rolling?

Several steps:

1. **Build into the manager and executive performance management process:** This includes the expectation, goals, and metrics of increasing employee wellbeing and resilience, employee net promoter scores, and engagement scores. Simple questions can be added to the customary annual surveys to measure employees' assessment of their manager's resilience and the degree to which their own resilience has been trained and valued. Trumpet successes of leaders and employees who demonstrate supreme resilience and demonstrably uplevel the skill level of their staff to be more resilient.

2. **Budget and resources to supply the tactical tools and training to drive those scores:** Direct manager-led training in Mindfulness is key… To drive that, top management and HR can establish a simple dashboard that shows which managers rolling up to the executive team have timely completed their direct manager-led resilience training. "What gets measured gets done," and just one dashboard will quickly create a healthy competition among mid-level managers to lead the training to completion.

Couple that with a Communication Strategy. The CEO and their direct reports can launch a simple concerted schedule of town hall mentions, all employee emails, events, etc., ideally populated with personal, real-life anecdotes about how a particular tool or technique helped that executive navigate through crises in their careers.

3. **Culture and Modeling:** The top executives and their direct reports need to authentically embrace and model resilience –and that may mean they will need training themselves, and receive candid real-time feedback when they model less-than-ideal resilience in moments of great challenge. Many of the most successful leaders will already have developed mental resilience and skills for shepherding teams through periods of great stress (or they wouldn't be in those roles), but all of us could benefit from formal refresher training and practice. At one company I saw the CEO modeling simple empathetic behaviors such as applauding risk-taking and constructive learning from mistakes, sending personal notes to staff, measuring individuals a full 50% on how they worked in the team and only 50% on what they achieved, etc. That modeling and unmistakable cultural mandate quickly led other execs, and then the other 85,000 employees in the company, to do the same.

This interview has been edited for length and clarity.

Follow Len on LinkedIn

"I've been a firm believer that a leader's primary responsibility is to increase the skills and capabilities of their staff… what makes a team great and greatly effective is where everyone has superb EQ, relationship, and stress management skills, which they can then deploy no matter what the crisis happens to be."

TPRM & Boards: Regulatory Change is Coming

TPRM compliance demands are impacting more global companies than ever before. Board directors need to consider a strategic approach.

Third-party risk management (TPRM) presents board directors with a great deal of complexity today, and that complexity is increasing. Depending on the industry, its supply chain, and its home country, a company will need to engage with a growing number of rules that require enhanced board oversight of more robust TPRM programmes. Some board directors are also finding they are faced with increasing levels of personal accountability, too.

For example, in the UK, The Modern Slavery Act of 2015 is about to be updated, with the contents of corporate disclosures made compulsory, the creation of a mandatory government registry of statements, and the introduction of civil penalties. The board will need to sign-off the new mandatory disclosures. Already, according to recent research by the Financial Reporting Council, the CEO and/or board Chair signs-off on 80% of today's modern slavery statements – where the content is not mandatory – with a further 12% of statements being signed by a board member other than the CEO or Chair. However, the introduction of mandatory content and civil penalties will increase the pressure on boards to get this right.

UK financial services organisations are also having to contend with new outsourcing rules and recent rules about operational resilience for third parties. These new rules create enforceable personal accountability for the senior managers named to be in charge of outsourcing and operational resilience. In the EU, the new Digital Operational Resilience Act (DORA) will bring in a host of new requirements around managing technology, data, and third parties for financial firms. And in the US, the banking regulators have combined forces and are working on finalising their Proposed Interagency Guidance on Third-Party Relationships: Risk Management, originally published in July 2021.

Globally, modern slavery rules are being upgraded too. The EU is expected to pass its own set of regulations this year, and Germany is implementing its new supply chain act, which requires due diligence and mandatory reporting, and provides for administrative fines for individuals as well as organisations. Australia is set to review its modern slavery regulations, too. The general direction of travel for new rules is to tighten things up – the need to make its modern slavery legislation more robust was actually a campaign issue in Australia, for example. The contents of modern slavery statements are being made mandatory, and transparency is being increased by having them compulsorily lodged in government registries. Penalties for non-compliance are also being included where they have not been before. Companies can expect modern slavery rules to evolve in jurisdictions where they already exist, and to be introduced into new jurisdictions over the next few years.

> "Companies can expect modern slavery rules to evolve in jurisdictions where they already exist, and to be introduced into new jurisdictions over the next few years."

More TPRM Involvement for Boards

With this velocity of regulatory change, and volume of new requirements emerging around the globe, board directors of companies with impacted supply chains, or who are vendors within impacted supply change, face real challenges. Certainly, board directors need to ensure their organisations are compliant with all the new, relevant regulations. At a minimum, this will include ensuring that the company's TPRM programme is functioning properly, as well as meeting reporting requirements. For many boards, this will mean introducing due diligence programs in their organisations for the first time. In some jurisdictions, there is personal accountability within senior management around this.

Board directors will also need to sign off on new mandatory modern slavery statements – and be confident that what is in those statements is truthful. For boards, this will require new levels of transparency into, and governance of, TPRM programmes.

Also, thoughtful boards will recognise the increasing attention being paid to issues such as modern slavery and bribery & corruption within the environmental, social, and governance (ESG) movement. In the UK, TPRM and operational resilience are being tied to the ability of financial firms to provide services to vulnerable people in times of crisis. So, increasingly, TPRM is being tied to ethical issues by regulators, the media, and customers. Negative news headlines and social media posts can deliver substantial reputational damage to all kinds of companies, which boards will want to prevent, if at all possible.

Rethinking Board Engagement

In light of these pressures, it makes sense for boards to take a more strategic approach towards their third-party risk management compliance responsibilities. Of course, boards need to meet the specific requirements of individual jurisdictions, but it is much easier to do so if a strong framework is already in place. Then such change becomes an adjustment, rather than a fundamental reworking of processes. Taking a more strategic approach also enables boards to drive more value out of the compliance infrastructure they are putting in place – boards can ask for the data they want for decision-making, as well as the data they need to meet regulatory obligations. So, what should such an approach look like? Below are 7 key suggestions for board directors to take to build a more strategic approach to TPRM:

1. **Understand the overall TPRM landscape** – Individual board members need to appreciate the TPRM context within which the organisation operates. For example, board members should be aware of how many third-party relationships the organisation has, the nature of those relationships, and what key dependencies there are on third parties to deliver products or services. Boards should also be aware of compliance requirements around TPRM and related areas such as modern slavery and bribery & corruption that are relevant to the company. In addition, boards should be informed about third-party risk management issues that have arisen at competitors, or at organisations with similar types of dependencies – such as cyberattacks, compliance breaches, and contract issues. These can help inform the board's TPRM strategy. Of course, board members should also understand the organisation's overall TPRM programme, and historical challenges.

> **"A negative event is more likely to 'stick' to the organisation – it will be accused of non-compliance in the media and by stakeholders, rather than the third party."**

2. **Make TPRM oversight a regular part of the board's rhythm** – Some boards assign TPRM responsibility to the risk committee or to the audit committee so that it becomes part of the normal board processes around risk management. In overseeing TPRM – either as a whole board or within a committee – board directors should consider:

- Confirming that third-party risks are managed in a manner consistent with the organisation's strategic goals and risk appetite – for example, that the TPRM programme has the right talent and resources. Organisations may want to consider creating a specific third-party risk appetite and set tolerance levels

- Reviewing and approving the organisation's TPRM policies, and related items such as modern slavery and bribery & corruption policies

- Reviewing key indicators that reflect the health of key or critical third-party relationships on an ongoing basis

- Ensuring that management addresses a significant deterioration in the performance of a third party, or an increase in risk, as reported by senior management or visible through key indicator reports

- Periodically evaluating the rhythm of activities around TPRM to ensure that it is adequate – that it is addressing any compliance requirements, but also that it is supporting the organisation in achieving its strategic goals, and that it is protecting the organisation's reputation

For activities that should occur on a regular basis, boards should schedule these in, along with presentations from the business where that would be helpful.

3. **Obtain regular information on compliance within third-party relationships** – Boards should never assume that outsourcing a process to a third party means that responsibility for regulatory compliance is outsourced too. Many financial services regulators make this explicit in their rules. However, no matter the industry or jurisdiction, boards should assume their organisation still holds responsibility for compliance and receive regular reporting to confirm that third parties are meeting their compliance requirements. Even if this is not an explicit requirement, it is a good way to reduce third-party risk, because a negative event is more likely to "stick" to the organisation – it will be accused of non-compliance in the media and by stakeholders, rather than the third party.

4. **Provide overall scrutiny of critical third parties** – Some industries, such as financial services, may already require board scrutiny of TPRM programmes in some jurisdictions. Regulators use different labels for this type of third party – for example, the UK regulators talk about "material third parties" – which provide business services or products which are fundamental to the organisation's processes. Generally speaking, issues at these critical third parties are more likely to impact the organisation in ways that make it much more difficult for it to achieve its strategic goals. For example, a cyberattack at a supplier of key product components could disrupt the organisation's manufacturing process for days or even weeks. Knowing that the supplier meets industry standards for cyber security, and building an operational resilience plan in case of disruption, will ultimately make the organisation better able to withstand such an event.

5. **Require board approval of new contracts for certain third-party relationships** – Contracts that are of strategic importance to the ability of the organisation to achieve its goals should be reviewed by the board before they are agreed upon. For example, boards should seek to make sure the third party

is financially robust, that it can deliver on any compliance requirements, and that it is a good fit for the organisation's needs. Boards might want to pay particular attention to data protection and data security arrangements, information and cyber security, business continuity, operational resilience, and how the organisation would exit the relationship under stressed circumstances – for example, if the third party's facility burnt down in a fire.

6. **Ensure a periodic independent review is conducted, and that the results are reported to the board** – In particular, boards should make sure that:

- Third-party relationships align with the organisation's overall strategic goals
- Risks in third-party relationships are identified, measured, monitored, and controlled
- Concentration risks are identified, monitored and managed. This is the risk that through having multiple third party – and nth party – contracts with a third party, an organisation may become inadvertently very reliant on that third party so that a disruption at that third party would have an outsized impact on the organisation. Geographic concentration is another form of concentration risk
- Material breaches and disruptions are being managed successfully
- The TPRM programme has the right talent and expertise to perform risk assessments, due diligence, contract negotiation, and ongoing monitoring of third parties
- Accountability for the management of third parties is transparent within the organisation
- Conflicts of interest are being managed appropriately
- Training to support TPRM is adequate across the organisation
- Overall, boards want to be sure that management oversight of the TPRM programme is effective and that the programme is functioning as it should be

7. **When needed, obtain an external review of the TPRM programme** – Having an external review of the TPRM programme by external auditors or consultants, for example, can help give boards the assurance they need about the quality of their organisation's programme, and provide insight into areas for improvement or best practices to aspire to.

To implement all of the above suggestions, boards will need to receive regular reporting on TPRM from all three lines of defence. Boards need to ensure that the reporting they receive is clear, consistent, robust, timely, and actionable. It should contain the right level of technical detail to facilitate effective oversight and challenge by the board. To do this, the board needs to understand the data that is available to it, and what limitations this might impose on having the kind of clear view that would enable the board to carry out the discussed activities.

Boards also need to strike the right balance between granular information on individual third-party relationships, and more holistic data covering things like concentration risk and inherent and residual risk positions. Boards – along with senior management – need to be able to spot important TPRM data trends that they may need to act on.

Overall, boards that want to take a more strategic approach to TPRM may wish to perform a gap analysis, to identify the difference between the data they need – including timeliness, quality, and provenance – and the current data "state of play." Boards can then work with senior management to develop a roadmap to develop the required level of TPRM reporting for the board.

The Ethical Board and TPRM

Best Practices for Taking an Active Role, Reducing Risk, and Navigating Compliance

Barbara-Ann Boehler
Regulatory Compliance Analyst

Events over the last few years have challenged organizations like never before. Epic weather events, global pandemics, geopolitical unrest, and cybersecurity concerns, to name just a few, have a wide impact and illustrate just how intricately connected the world is. Managing risk is an increasingly complex effort in these volatile times and is top of mind for Boards of Directors across every industry. Organizations need to be concerned not only with their own company's risk profile but also the risk profile of the third parties with whom they partner. Boards are well aware the actions of an organization's third-party vendors reflect upon them and impact the success and reputation of their business.

No organization is an island, third-party relationships – which include suppliers, outsourcers, licensees, agents, distributors, and vendors are an essential element of any functional business ecosystem. When third-party relationships are effective, the organization benefits in innumerable ways. Conversely, when the relationships fail, those failures are fraught with risk for the organization. In this era of reliance on social networking, and the swiftness of a viral story – third-party relationship failures have the potential to impact organizations on an epic (and very public) scale.

Third-Party Risk Management: The Process

Third-party risk management (TPRM), when adopted and operationalized by an organization, helps identify, evaluate, monitor, and manage the risks associated with third-party relationships. To be competitive, organizations employ strategic and operational reliance on third parties. With this reliance comes increased risk, which must be identified, understood, and managed. TPRM is often a complex exercise. It is not unlikely for organizations to have many thousands of third parties often with unique risks and challenges.

To further complicate TPRM, regulators across industries and jurisdictions are also focused on third-party risk. While organizations might outsource a task, they cannot outsource their responsibility. Increased regulatory scrutiny, however, is just a symptom of the underlying issue – the way organizations do business is evolving dramatically and rapidly. And with this, the way they manage risk and govern their extended enterprise needs to evolve quickly, too.

TPRM is a relatively new discipline and companies are at radically different stages of maturity, depending on their industry, size, and culture. From a discipline that has evolved largely from siloed and ad-hoc processes, there's a growing recognition that a more cohesive, standardized, and enterprise-wide view of risk is required.

The Role of the Board

Progressive boards are recognizing that an increased focus on third-party risk makes good business sense, given the importance of third-party relationships in the organization's overall strategic approach.

In fact, Deloitte states that, "those organizations that have a good handle on their third-party business partners, cannot only avoid the punitive costs and reputational damage, but also stand to gain competitive advantage over their peers, outperforming them by an additional four to five percent ROE [Return on Equity], which, in the case of Fortune 500 companies, can mean additional EBITA in the range of $24-500 million."[1]

But there's more to board oversight than fiduciary duty. Who organizations do business with matters and can have far-reaching implications. Boards that promote ethical cultures and the 'tone from the top' that they and their C-suite deliver are integral to ensuring that the business acts with integrity and keeps bad business practices – such as corruption, human rights abuses, or environmental crime – from their wider business relationships and supply chain. Put simply, boards are not fulfilling their oversight responsibilities if they don't take measures to lead ethical business practices across the enterprise, which includes the third-party ecosystem.

Research indicates that an organization's ability to effectively mitigate third-party risk is tied to greater board involvement. In Aravo's 2021 TPRM Benchmarking Survey, a strong correlation was reported between board involvement in TPRM strategy, resilience, and maturity.[2]

TPRM Best Practices

An organization with a mature, agile TPRM strategy has immediate enterprise visibility into third-party risk at every level: an overview of the inherent risks across the third-party portfolio, a robust risk profile of each individual entity, and insight into third-party performance related to specific contracts or key performance indicators (KPIs). To achieve this level of insight and confidence, organizations can implement a few interrelated best practices:

The federated approach: A balance of centralized risk management responsibility with participation from both business owners and relationship managers allows organizations to standardize TPRM policies and procedures. A federated TPRM system acts as a single source of truth across the enterprise and can generate insights the board needs for high-level oversight, as well as be alerted to risks that might be overlooked when information is in silos. For example, in a disconnected system, leaders may not realize that a third party has relationships in multiple critical areas and therefore may underestimate the risk they present to the organization. If that third party crossed a risk threshold (like a change of ownership that signaled a corruption risk), it's possible that not everyone would be alerted.

Management of the entire life cycle: Assessing third-party risk isn't a 'one and done' exercise. Between onboarding and termination, a third party's risk profile can change, or they may fail to meet contractual obligations and have to go through a remediation process. Juggling documents and spreadsheets for ad-hoc TPRM processes or cobbling together disconnected silos of TPRM practices won't provide the enterprise visibility an organization needs to fulfill its oversight obligations. The organization would also be wasting valuable resources trying to analyze and report on data across the third-party ecosystem while increasing potential exposure to unforeseen risks.

Enterprise visibility: While the board sets the tone for creating a culture of ethical behavior and accountability, multiple stakeholders are responsible for executing, sustaining, and auditing TPRM policies and procedures. Most of those stakeholders have other responsibilities as well, so it's important that they can easily and securely receive notifications and view the data they need based on their roles, whether in a high-level dashboard, detailed reporting or by drilling down into specific records. By employing a centralized system of record, TPRM is able to deliver an enterprise view of the data, based on the user's role in the organization.

> **"Boards are not fulfilling their oversight responsibilities if they don't take measures to lead ethical business practices across the enterprise, which includes the third-party ecosystem."**

[1] Deloitte. "Third-Party Governance and Risk Management: The Threats are Real." Global Survey 2016.

[2] Aravo Solutions. "Gaining Clarity: A Better Line of Sight into Third-Party Risk." 2021 TPRM Benchmarking Survey.

Secure agility: In addition to changes in risk profile, internal policies and regulatory requirements also change, so organizations need to be able to adapt without prolonged or complicated projects. For instance, the General Data Protection Regulation (GDPR) that came into force a few years ago meant that organizations that hold or processed personally identifiable information for EU citizens will have needed to evaluate their portfolio of third parties to identify which came within the scope of the regulation, assess them for their compliance posture, and ensure reporting and escalation processes were in place for reporting to the regulators. With the advent of any new regulation, organizations can't afford to be locked into rigid systems.

Building Effective TPRM Oversight Best Practices

1. Identify your risk appetite

As part of their oversight responsibility, board members should agree on and articulate what an acceptable risk is and what isn't. Obviously, there are third-party behaviors that can't be tolerated, such as clear ethical and criminal violations, but somewhere between the impossible goal of zero risk and unacceptable behavior, there is a point at which the organization is willing to accept the risk-to-value ratio.

Understanding and evolving the level of acceptable risk requires input and counsel from board members. Larger or more complex organizations may determine varying risk appetites based on factors such as geography, industry, and division of risk type. Certain kinds of risk (such as establishing a critical third-party relationship in a country with a high incidence of corruption) call for greater due diligence than others (such as warehouse janitorial services). These thresholds should be built into the TPRM platform to trigger automatic warnings and remediation when they are exceeded.

2. Create and support a governance structure

Consistent policies and procedures make it possible for an organization to identify, analyze, and manage risk in a way that can be communicated both internally and externally. To oversee the execution of policies and procedures, many boards are appointing a specific director as the point person for third-party risk. Some are also establishing managing boards in specific regions or business units to reinforce both the guidelines and the culture of ethical behavior and compliance.

> "Even with the most robust system for managing and understanding third-party risk, the board needs to maintain ongoing oversight."

Balancing centralized risk management responsibility with participation from business owners and relationship managers allows organizations to standardize TPRM policies and procedures without having to run a 'risk business unit.' By investing in technology that automates processes and empowers employees to manage risk in a federated system, organizations can impose centralized control without sacrificing overall productivity.

3. Clearly define roles and responsibilities

With an overall culture of compliance, there should be clear expectations and accountability across all three lines of defense:

1. Those who own and manage risk (e.g., a business owner or relationship manager),

2. Those responsible for overseeing risk management or compliance (e.g., a risk and compliance executive) and

3. Those who validate compliance with third-party policies and procedures (e.g., internal auditors).

By working collaboratively, these roles efficiently provide the needed third-party risk documentation and reporting, oversight and accountability, and independent reviews. When roles aren't clearly defined, TPRM may not be given the priority and attention needed to protect the organization from external risk.

4. Review regularly

Even with the most robust system for managing and understanding third-party risk, the board needs to maintain ongoing oversight. Management should be expected to report on critical KPIs and significant changes, remediation/residual risk, and critical relationships that could impact the organization's financial or reputational performance.

The board should review the overall TPRM strategy annually to ensure that it stays current with organizational goals and the business ecosystem. While it shouldn't require a complete overhaul, factors such as a change in risk appetite, new initiatives that introduce new risk domains, and changing legislation or enforcement guidance will require adjustments to TPRM policies, procedures, and processes.

Regulatory Expectations of Board Members

Recognizing the ethical leadership role of board members, regulators are increasingly holding them accountable for poor behavior, which could lead to board shake-ups and even personal liability. Board minutes should reflect board input, review, and approval of TPRM strategy, as well as remedial actions. Regulators expect to see the following information included in board minutes of compliant organizations:

- A record of attendance and participation in regular third-party review meetings
- The methodology for categorizing critical activities
- The approved plan for employing third parties for critical activities
- Third-party contracts for critical activities
- A summary of due diligence results and ongoing monitoring of third parties involved in critical activities
- Results of periodic internal or independent third-party audits of TPRM processes
- Proof of oversight of management efforts to remedy deterioration in performance, material issues, or changing risks identified through internal or external audits
- Embedding TPRM governance in the organizational culture

The role of the board in gaining acceptance for a TPRM governance program can't be overstated. Without organizational buy-in, it's unlikely the program will deliver the desired value and results. Creating and sustaining this buy-in requires ongoing support and monitoring as the program is rolled out and over the long term. To help ensure the governance program is being accepted by the organization and delivering value, boards should:

- Provide the right resources for the team implementing the governance program
- Encourage effective collaboration between risk, compliance, procurement, and the business, among other teams
- Reward the achievement of TPRM organizational metrics (such as through MBOs), when appropriate
- Implement high-quality training for employees involved with third-party relationships
- Communicate the importance of TPRM across the enterprise, starting at the top
- Invest in a technology platform that reflects best practices and enables effective collaboration, communication, and relationship management

Overseeing a strong TPRM program demonstrates the board's commitment to the financial and ethical integrity of the organizations that they lead. It helps to ensure their organization can deliver the value it should be creating for customers, improve relationships with third parties and key stakeholders (such as industry regulators), and uphold fair business practices.

> **"Somewhere between the impossible goal of zero risk and unacceptable behavior, there is a point at which the organization is willing to accept the risk-to-value ratio. Understanding and evolving the level of acceptable risk requires input and counsel from board members."**

About the Author:

Barbara-Ann Boehler is an attorney and adjunct lecturer with over twenty years of compliance experience and teaches "Compliance Practice Skills" at Suffolk University Law School and Boston University Law School. Barbara-Ann formerly served as the Director of Programming and Education at Compliance Week, Securities SME at Wolters Kluwer Financial Services, and Global Chief Compliance Officer for Arete Research, a limited-purpose, FINRA-registered broker/dealer specializing in equity research. Barbara-Ann also held compliance roles at Fidelity Investments, JP Morgan Invest, Standish Mellon Asset Management, and Babson Capital Management. Barbara-Ann holds a BA from Suffolk University, a JD from Suffolk University Law School, and an LL.M. from Boston University School of Law.

INTERVIEW

With New ESG and DEI Rules Comes Additional Complexity – and Opportunity – for Board Directors

A conversation with DeAnne Dupont, Independent Director at DWS Trust Company and a Nonprofit Advocate

DeAnne Dupont
Independent Director at DWS Trust Company and a Nonprofit Advocate

Thank you so much, DeAnne, for speaking with us. Could you please introduce yourself and your role?

Sure. My name is DeAnne Dupont and I serve on one corporate board, DWS Trust Company, and several nonprofit boards. My roles on the corporate board – in addition to serving on the board – are chair of the audit committee and member of the investment committee.

As to the nonprofit boards, I have various roles. For Boston Building Resources, I'm the treasurer and I serve on various committees, such as the transition committee, the finance committee, and the development committee. For Goddard House Assisted Living Facility, I am the assistant treasurer and am on the audit and finance committees, as well as the building committee. I'm also on the board of the Arlington Chamber of Commerce. In the past, I have held various other nonprofit board positions, including being the board chair and serving on the executive committee.

You have many different board positions, and it seems like a lot of them are financial and audit board roles. How does this fit in with your background?

I was a managing director, the treasurer and controller of Babson Capital Management, which is now called Barings, LLC. In these roles, I oversaw all financial reporting and treasury functions, as well as incentive compensation and several other areas. For several years, in addition to the aforementioned, I was also the treasurer of a mutual fund group. My background is that I am a CPA and was a manager at Deloitte. So, my board roles tend to leverage my financial background.

You have a lot of experience sitting on boards, but could you talk a little bit about your experience reporting to a board?

Sure. As treasurer and controller of Barings, LLC, I reported to the board of managers, the executive committee, and the audit committee. I also participated in most of their meetings. Additionally, I sat on various committees of the firm. My reporting functions were primarily focused on the financial performance of the company and executive incentive compensation. So, I had to be prepared with many answers and sometimes it could be intimidating – not only because I was not actually on the board, but also because I was the only female in the room. This was a challenge as I felt the bar was higher for me. It may not have been, but that's how I perceived it. So as a presenter I wanted to know my information and present it effectively.

Also, as treasurer of the mutual fund group, I was reporting to the board of trustees. Although the role was a finance one, it also leaned heavily towards compliance because it is a heavily regulated industry with complex tax laws. Being very knowledgeable on the subject matter and anticipating questions was extremely important.

> "I am very interested in how we can ensure that we are getting that needed equity, diversity, and inclusion in the boardroom."

Since you've sat on both sides, are you more demanding of those who are coming before you to provide information to the board?

Actually, I am demanding, but I also feel that I'm understanding as well. So, even though I may ask questions and the individual presenting may not have the answers to the question, I understand and don't expect them to have all the answers. What I do expect is that they'll come back to the board with the answers. I don't look negatively when somebody says they have to get back to us and that the information is not readily handy. I actually appreciate that.

If you're expecting an individual to have all the answers, they're going to spend so much time preparing for the meeting they won't have time to do their actual job. This is why I think it's better to build a culture where people can return when they have the answers.

What does the landscape for board governance look like currently?

Overall, there has been much improvement, but there is still a long way to go as the governance landscape keeps changing and getting more complex. Now boards and their organizations have environmental, social and governance (ESG) policies and diversity, equity and inclusion (DEI) policies incorporated in their board governance. More policies mean more reporting to and oversight by a board.

An example of complexity is ESG and related reporting. A company may be reporting ESG at one level, but they should also be drilling down further into their supply chain. I think it is a challenge for companies to drill down and incorporate information on their suppliers into their reports. Deciding how and what to report is already and will continue to be extremely challenging. Gathering the information for the reports is challenging.

The U.S. Securities and Exchange Commission (SEC) will be adding climate-related disclosure requirements for public companies. Additionally, the International Sustainability Standards Board (ISSB) is proposing global standards for general sustainability-related and climate-related disclosure requirements. For boards, this means that their companies will require additional data gathering in order to provide the information needed for the disclosures accurately.

> "If you're expecting an individual to have all the answers, they're going to spend so much time preparing for the meeting they won't have time to do their actual job. This is why I think it's better to build a culture where people can return when they have the answers."

Where would you like to see the regulatory landscape head in the future?

There's room for improvement around equity in the boardroom, as part of DEI corporate policies. Responsibilities of the board include leadership and setting the "tone at the top." There's often a focus on diversity and inclusion, but the equity part ties all three together. Part of equity is providing opportunity. Boards should lead their organization's DEI initiative by example.

I am very interested in how we can ensure that we are getting that needed equity, diversity, and inclusion in the boardroom. An example is about a year ago, I recommended someone for a nonprofit board. She was elected and is an outstanding board member and brought more ethnic diversity. She then brought someone else onto the board that brought in increased diversity.

People tend to bring in other people that look like them. And so, by bringing in diversity, people start getting used to diversity. As a result, I believe that more diversity and inclusion will happen organically once it gets initial momentum, as it did in this example.

Are there specific issues or types of risks that you think boards should be paying more attention to in the future? Maybe things that aren't quite yet on their radar?

I think there are many risks that are already on boards' radars, but perhaps not as fully as I think they should be. One of great importance is the impact of climate change. This includes both the general impact and more specifically, the impact of what we want and what we do to the environment. Corporations and their boards are looking to sell their products and be profitable. And I get that, but they also need to look at the impact of their actions on the environment. For example, of course a retailer wants to sell clothing and to sell more clothes. But do we really need the volume of clothes they sell? Retailers should also look at what people do with their clothing when they no longer want it. They should ensure that there is an easy way for consumers, when products are no longer needed and wanted, or when they break, to return them to the manufacturers at no additional cost to the consumer. Alternatively, there needs to be a process to receive these discards into the waste stream that is better for the environment – so they can be repurposed, reused, or made into another product.

Boards need to consider the impact of their products on the environment, and the environmental impact of the behavior their companies are encouraging because they want profits – while simultaneously keeping in mind the interests of the shareholders.

As someone who has sat on nonprofit boards, what are some of the differences in priorities between the nonprofit board and the corporate board?

The smaller nonprofit is focused on its mission and that's understandable – they have a mission and they see the need out there. However, this means that sometimes they are not focused on the fact that they are a business. A nonprofit is a business and they need to be willing to spend some of their hard-earned funds towards other needs, such as the back office or compliance and governance. Actions like ensuring their financial stability are not always on their radar.

One of the things I do even before I join a nonprofit board is that I review their financial reserves. I want to see if the nonprofit is in a stable financial position or whether they're living, as one might say, "paycheck to paycheck," because that's not healthy for a nonprofit. They need to develop financial reserves. Overall, most nonprofit boards need to have an even greater focus on board governance, particularly the smaller ones.

Is there anything else that you would like to share about your board experience?

I think being on a board can be fulfilling. You can bring your expertise to an organization, bring a different viewpoint and perspective. This is true for all types of boards, both corporate and nonprofit. Diversity can mean so many things, and some of it is your background, which can be extremely important. Organizations need that diversity of knowledge and background to have an effective board, no matter whether it's nonprofit or for-profit.

> **"Boards need to consider the impact of their products on the environment, and the environmental impact of the behavior their companies are encouraging... while simultaneously keeping in mind the interests of the shareholders."**

About the Contributor:

DeAnne Dupont, CPA, is a nonprofit advocate serving on several nonprofit boards. Most recently she leads the nonprofit, Food Link, Inc. of Massachusetts as its Co-founder and for nine years serves as its Executive Director/CEO and President. DeAnne brings her financial services, finance, and business expertise to DWS Trust Company, a wholly owned subsidiary of DWS Investment Management Americas, Inc., where she serves on the Board of Directors, and as chair of the Audit Committee and member of the Investment Committee.

Outside of her business career, DeAnne leverages her leadership capabilities to positively benefit the community. DeAnne is currently on the board and the treasurer of Boston Building Resources, and is on the board and the assistant treasurer of the Home for Aged Women, Inc. d/b/a Goddard House. She further strengthens her participation in her community as a board member of the Arlington Chamber of Commerce (Chamber).

ROUNDTABLE

Board Members:

It's Time to Take an Active Role in TPRM and Cyber Programs

A conversation on the importance of board engagement with

Nick Donofrio
IBM Fellow Emeritus and former
Executive Vice President of
Innovation and Technology

Christos Kalantzis
Chief Technology Officer
at SecurityScorecard

Eric Hensley
Chief Technology Officer &
Chief Security Officer
at Aravo Solutions

Why do boards need to be thinking about third-party and cyber risk?

ERIC: Risks in supply chains never get any easier. Boards are often not even thinking about that. If they think about supply chain risk at all, they're thinking about disruptions to whatever their company is producing with their supply chain, as opposed to adjunct risks that have these related, but very different, bad outcomes. And so, broadening your imagination concerning what's going on in your supply chain from a risk point of view is really important.

NICK: One of the risks we're forgetting is that directors of boards don't understand the risk for themselves. They have no sense of the consequences of their lack of knowledge or lack of action. And that's already starting to change. You see governance from various authorities coming into play that says, in the end, board members are responsible for an incident. It's your fault that you didn't know, it's your fault that you didn't ask the questions.

The SEC, for example, is starting to ask questions of boards like, what did you do about that breach? When did you know about it? Did you understand the consequences? Where was your duty of care or service? Where was your duty of loyalty? Regulations like this are continuing to come and you better wake up to it… So, I'm worried about a lack of understanding of third-party risks and inherited risks.

What do you think the hurdles are when it comes to understanding?

ERIC: There's governance now for board members and directors. It's not going to be good enough to not know and use that as an excuse for why there wasn't any action. The upside of that is all you need to do is ask. This might just be having a board member ask a question in a board meeting about what's being done about third-party risk or cyber risk. Simple little steps. This could open up an enormous amount of help for these problems.

NICK: It doesn't require you to be a cyber expert… It's simple, logical questions that you should be asking.

CHRISTOS: I've always been amazed at how boards can move mountains and change the trajectory of a company. And they do it by asking very simple questions. Ask "how will we avoid being breached?" The person asking doesn't have to be a cyber practitioner. That will grow into programs, motions, evaluations, and improvements because a board member had the courage to ask.

NICK: Build up your courage as a director or as a trustee. There are a lot of ways for you to become more educated and comfortable. Because in the end, regulators are going to be coming for you, incidents are going to be your fault… especially in the space of data, cyber, and technology.

CHRISTOS: And the regulators have recognized that boards are not asking these questions. The regulators are now asking boards to prove things. Declarations may be optional now, but read the tea leaves; within 12 to 18 months, I believe that's going to become a required declaration of your security posture.

NICK: It's not a deep, dark set of secrets. There are always going to be issues. There are going to be Solar Wind-type of issues because that's just the way technology evolves. That's not necessarily the problem. The problem is what did you do about it? Because once they're reviewed, once the government looks at the breach, they're going to then go back to the board. So, as the government becomes more informed on what it's doing about these breaches, you as a director better take your game up. You better start asking these simple questions, see something, say something. It's no more complicated than that.

"Build up your courage as a director or as a trustee. There are a lot of ways for you to become more educated and comfortable. Because in the end, regulators are going to be coming for you, incidents are going to be your fault."

– Nick Donofrio

How do board members dig deeper into finding out what risks they should be paying attention to?

ERIC: When I talk to board members, the answer they get is along the lines of, “we’re working on it but wish we could get more attention.” Many times, they already have tools, automation, and a whole risk management process, but it’s buried and doesn’t get applied appropriately across all risk areas. So, when you’re asking this question, you want to look for who in our company is the person who’s on this. A lot of times they’re going to be dying to talk to you because they’re spending all day worrying about these risks. Second, you want to ask them if they’re appropriately resourced for what they think these risks are. Have them explain it at a high level.

NICK: It goes back to the director or the trustee telling their teams to not be afraid to say something… There are people inside the company who are basically hemorrhaging, waiting to have somebody listen to them and just give them a voice to be able to explain what’s going on. And you become a much more informed director and trustee by letting them do that.

CHRISTOS: This interest from boards immediately gives a voice to the team and their morale will go through the roof. They know their work matters and the board wants to hear about it. It gives them a renewed sense of purpose and productivity increases… Providing that voice has a tremendous impact both on the company, its business, and the team members as well.

> **“As long as it’s at a reasonable level of detail, you want to make sure that the board understands the risks that you’re worried about first. But don’t get too bogged down on details- think about outcomes rather than processes… and then talk about that over time.”**
>
> – Eric Hensley

What kind of data should be reported and presented to the board?

CHRISTOS: Step one is ask the question. Step two- follow up, look at a trend. Show me the issue over time. Ask what’s the KPI? What are we measuring ourselves on? And show me how it’s improved to glean immediately if they’re moving in the right direction or not. If there isn’t that follow-up then it’s an empty question.

ERIC: I find that boards have a hard time with process descriptions, which is really what your risk folks want to convey. As long as it’s at a reasonable level of detail, you want to make sure that the board understands the risks that you’re worried about first. But don’t get too bogged down on details- think about outcomes rather than processes… and then talk about that over time.

Why is it important to create a culture that encourages people to come forward about risks?

NICK: As a board member, you want to build an environment where people can be forthright. The only way that works is if risk teams are willing and comfortable with speaking up to help boards understand if there is trouble. If there is fear of being forthcoming it stops boards from actually understanding the problem in a timely way. So, culture is very important for you as a board member to ensure that people are comfortable with coming forward. If people aren’t empowered to do this, you’re never going to hear their concerns.

ERIC: People will hide problems if they feel like they’re going to get in trouble. If someone’s going to get in trouble because they revealed a risk, it will have a way of either never really getting answered or never really getting asked. Even if nothing is being done to mitigate a risk yet, that answer and information are still better than no feedback at all. But it’s often the responsibility of boards and the top executives to foster that culture.

If boards are not engaged in cyber risk in particular, or not asking the right questions, what are the consequences?

NICK: If they’re not asking these questions then they’re hanging on a thread of regulatory supervision, or they’re going to go out of business at some point in time. They’re going to fall apart because there isn’t a company of any size that isn’t plugged in and doesn’t have inherited cyber risks.

CHRISTOS: There’s no such thing as a tech company anymore, all companies use tech, all companies are tech companies, it’s just a reality. All companies have an attack surface.

NICK: Even if you’re doing the minimum amount of protection you’re tremendously lowering the probability of being breached or increasing the probability of being safe. It’s not hard, but someone needs to ask the question and nudge the company in that direction. And in the absence of it, someone else will do it for you, either by overtaking you business-wise, or a regulator will come in and force you to take steps.

CHRISTOS: The tools exist to help answer these questions. Just give somebody the leeway to go out and research and figure out who the market leader is. All the data and services are there. There's no excuse to not do this.

ERIC: Companies use a lot of technology in their aggregate company, and they have a lot of suppliers. And it is simple logic, those suppliers are all technology companies too. That's a sobering thought for people. But we live in a sort of a golden age of automation. The point is to leverage automation to assess and manage the risk of the entirety of your supply chain for something like cyber risk, and in a scalable way.

What advice would you give to a new board member to help them get up to speed on third-party risks and make a difference in their business?

CHRISTOS: Be courageous, ask questions- it doesn't matter if you're not a subject matter expert in what you're asking- ask it anyways. Follow up, be active… You probably joined a board because you've been successful and have contacts to help the company. Use your network. But it all starts with having the courage to ask the questions.

ERIC: Being that friendly interrogator is valuable. You're not asking these questions because you're overbearing. You're asking because you want to make your business more agile and less risky. But keep the tone of it friendly.

NICK: Don't ever stop learning. You don't know it all, there's so much more to be done and there's so much ahead of you. So, as a director or trustee, don't just be onboarded, but continuously re-onboard yourself by continuously educating yourself. No one's expecting you to be the expert, but we are expecting you to be knowledgeable. We are expecting you to live up to that fiduciary responsibility, that duty of loyalty, duty of care. And learning about it should be fun. So, if you take it on from that perspective, I think you will be a happier, more effective director and trustee. And I think you will be richly rewarded.

This interview has been edited for length and clarity.

> "I've always been amazed at how boards can move mountains and change the trajectory of a company. And they do it by asking very simple questions. Ask how will we avoid being breached."
>
> – Christos Kalantzis

About the Contributors:

Nick Donofrio *is an IBM veteran who led IBM's technology and innovation strategies from 1997 until his retirement in 2008. He was vice chairman of the IBM International Foundation and chairman of the Board of Governors for the IBM Academy of Technology. Mr. Donofrio's most recent responsibilities included IBM Research, Governmental Programs, Technical Support & Quality, Corporate Community Relations, as well as Environmental Health & Product Safety. In addition, Mr. Donofrio led the development and retention of IBM's technical population and enriched that community with a diversity of culture and thought. In 2008 IBM elected Nick IBM Fellow, the company's highest technical honor.*

Christos Kalantzis *is the CTO at SecurityScorecard. He is an experienced leader, technologist, and blogger, and is interested in big distributed systems and how to build teams to implement and maintain them. Christos grew up in Montreal, Canada, where he started his career as a DBA for companies such as Matrox, CGI, Sync, and InterTrade. He moved to Silicon Valley where he built and led engineering teams for FireEye, Tenable, Netflix, and YouSendIt. He has worked on Cloud storage solutions for YouSendIt, before the term "Cloud" was popular. He is also focused on solving at-scale run-time databases using sharded RDBMS and NoSQL products and is an Apache Cassandra MVP.*

Eric Hensley *is the Chief Technology Officer at Aravo Solutions, where he manages all products, product strategy, and technical delivery of their solutions. With a career in supply chain solutions, Eric joined Aravo in 2008 and has pushed for innovation in managing new risk domains.*

INTERVIEW

Enhanced Board Reporting on Supply Chain Risk Is Essential

A conversation with John Bolla, Global Business Operations and Supply Chain Expert

John Bolla
Global Business Operations and Supply Chain Expert

Thank you, John, for joining us. Could you share your experience in reporting to boards?

I've had roles as a C-suite chief operating officer (COO) of two different companies. When I was a public company officer, I was also responsible for leading the board's compensation committee and their nominating and governing committees. Overall, I was very much accountable to the boards to report on performance.

Also, I was accountable to the boards on compliance. As a COO, I needed to inform the board about specific areas of performance improvement and compliance such as financial, environmental health and safety, and quality assurance. I was also accountable for compliance as it relates to delivery and performance to our customers. So, our role as leaders was to attend board committee meetings and board meetings, to report on various aspects of performance and address the concerns and challenges that the board had.

How do you approach reporting to a board, especially when it comes to risk?

Reporting risk to the board starts with how you manage risk within your own organization. Companies may have different labels for risk processes and different risk management frameworks, but all companies need to manage risk through identifying risks to senior management and the board, reviewing those risks on a regular basis, identifying mitigation for those risks, and then implementing those mitigations.

One of the challenges that most boards and organizations have is actually identifying risks before they become issues. Most businesses engage with risks long before they ever get to the board of directors – we reviewed risk, we managed risk and we mitigated risk, both residual risks and inherent risks to the business. We then rolled those up through the chief executive officer of the company. Then, those risks would roll themselves up to the board and we'd address them and discuss them with the board. Risks often turn into issues, so we also discussed issues with the board, too.

Are there best practices you can share?

One of the best practices that I've consistently both undertaken and seen at other companies is assessing risk against its likelihood to occur and the potential severity of the occurrence. Severity is defined as how significant the impact will be on the organization from a financial perspective, a safety perspective, a quality perspective, and various other aspects. The best practice is that you assign scores to both likelihood and severity, and then you place it on a heat map according to those scores.

With this approach, you can see the biggest risk impacts to your organization, so that you can be sure you're managing the biggest risks based on how severe they are and how likely they are to happen. For example, if a risk is very unlikely to happen, but has high severity, you may manage that risk differently than if it's very likely to happen with a high severity.

> "ESG committees want to be sure their companies are not just thinking about the financial reward, or delivering value to shareholders. Instead, they are looking at the impact their companies are having on their communities… and hopefully mitigating those risks…"

Boards often want to see how the organization is looking at severity and likelihood, and they also want to ensure that the business is capturing the largest risks to the organization. That's what I see as one of the best practices. And then secondarily, I've also mentioned not just identifying risks, but bringing forward mitigations to those risks and acting before the risks transform themselves into issues. It's easy to identify things that could go wrong, but boards want to see that you've mitigated those risks before they happen. So, that tends to be another best practice that boards engage with.

Are there specific issues or types of risks you think should be reported to boards more in 2023?

Boards are used to seeing financial risks and compliance risks from a quality perspective or a regulatory compliance impact perspective. However, what boards don't see as much – and I think they should be interested in 2023 and beyond – is reporting around environmental, health and safety risk. We've all heard of ESG – environmental, social and governance. However, before there was ESG, there was the environmental, health and safety aspect of risk and risk management for boards. We don't see that talked about as much today. However, over the last few years, I've seen boards be much more interested in environmental, health and safety risk aspects of companies, whether it's what we produce into the air, or what we put into the water, or the impact that corporations in general have on the environment and the risks associated with that. Boards are going to be much more interested in 2023 and beyond in environmental, health and safety risk.

Employee health is another area that boards are very interested in, in 2023 and beyond. It's very challenging to get employees to come to work during a pandemic. It's very challenging to retain employees once you hire them. Boards are now taking a great interest in making sure that we as leaders in organizations are looking out for the health of our employees. That's not just the physical health of the employees, but it's the overall health of the employees, including their growth and development. Boards are very interested in employee health and safety risk, not just from a financial perspective, but as a key way to help retain more employees.

Any other priorities?

There's also a social aspect. That's the S part of ESG, and every board these days has an ESG committee, which is ensuring that their companies are looking out for the impact that they're having on society. These ESG committees want to be sure their companies are not just thinking about the financial reward, or delivering value to shareholders. Instead, they are looking at the impact their companies are having on their communities, and they are assessing those social risks, and hopefully mitigating those risks before they manifest themselves into issues.

I think you'll see more board members in the future focused on ESG, and it's incumbent upon the leaders in the organization to make sure that they're identifying risks and managing risks in this space.

As a guy that's been in operations my whole career, I can tell you that I've sat in many board meetings where the expectation is that the supply chain is buttoned up: supply of product, supply of input materials, et cetera, is a standard ticket to the ballpark. That's what you have to do to run your business. But in today's current environment, supply chain risks are incredibly challenging and boards are taking a much stronger interest. Many

> **"Boards often want to see how the organization is looking at severity and likelihood, and they also want to ensure that the business is capturing the largest risks to the organization. That's what I see as one of the best practices."**

businesses are much more interested in the risks associated with the supply chain. They are looking two or three levels back into the supply chain to understand what are raw material risks, environmental risks, safety risks, employee risks, et cetera.

How do you see, or how would you like to see, supply chain risk reporting improve in the future?

I've been reporting on supply chain risks my entire career – prior to being a chief operating officer, I was a chief supply chain officer. And early in my career I worked in procurement, manufacturing and supply chain. I'm currently at a company that is entirely focused on supply chain from an end-to-end perspective in the healthcare industry.

We work hard to mitigate supply chain risks at the business level. We look at risk from a supply chain perspective and from a supplier aspect, and we always have done those things in the businesses. As an example, we always look at supplier relationship maps, supplier risk maps, and we take steps back into the supply chain to understand the impact that the supply chain could have on our existing business. We look forward in the supply chain to our customers to try to understand the impacts of supply chain disruptions on them.

I think generally executives need to be more vocal about the risks associated with supply chains. We should provide them with a supply chain view that'll give them an understanding of the impact that the supply chain actually has on the very basic foundation of running the business. We need to be managing fulfillment times from a supply chain perspective. We need to be managing back two or three steps into the supply chain to understand where our materials come from, and what the geopolitical issues are in those regions. What are the potential impacts on the supply chain from an employment and workforce perspective? How will these issues impact our ability to deliver to our customers through our own supply chains? Ultimately, how will that impact our customers, and then all the way to the ultimate consumer – the patients – that we serve?

Can you expand on this?

Boards need to see those risks on the same basis as other risks – through likelihood versus severity – so that they can help assess what the impact might be on their corporations, and the shareholders they represent. At the end of the day, boards need to pay more attention to supply chain risks. They should be demanding that supply chain and operations executives bring to them the same level of risk management and compliance data for supply chains as other areas of the company bring for their risks.

From a financial perspective, well-managed supply chains tend to be a lead-in to the successful financial performance of companies – at least, for those that are manufacturing and supply chain driven. As much as boards are interested in ESG, quality, compliance, and financial risks, boards need to increase their interest in supply chain risks. You only need to read the news or a website to understand that supply chain risks are substantially impacting companies around the globe today. Boards need to be paying more attention to supply chain risks, and demanding more insight from their supply chain executives about those risks and how they may impact their business.

> "I think generally executives need to be more vocal about the risks associated with supply chains."

If you had to pick one piece of insight on board reporting to impress on our readers, what do you think they need to know?

Oftentimes boards are only as knowledgeable as the executives that bring them the issues. There are some boards of companies that have deep subject matter expertise, but other times there are board members that are executives from other industries or other functions. I really think it's incumbent upon executives that report to the board to bring a level of detailed information on issues that enables the board to give back input. I've seen people treat reporting to the board as a necessary evil, as opposed to a collaboration, which is what it's supposed to be. Board members are there to impart their wisdom and their experience and share their knowledge, as well as to represent the shareholders. I think senior leaders and organizations need to work closer with boards to manage and assess risk, and either prevent issues from happening, or mitigate their impact. So, as it relates to board reporting, it's important that executives understand it should not just be about reporting. It's about sharing and collaborating to reduce or eliminate the risks, to prevent them from turning into issues and problems.

About the Contributor:

John Bolla holds extensive experience in global supply chain and business operations spanning several decades. John has led and developed manufacturing networks, supply chains, production planning, strategic supplier sourcing, inventory management, and logistics functions throughout his career at organizations such as GSK, Lantheus Medical Imaging, Adare Pharma Solutions and others. John holds a BS in Accounting and Business Management from the University of Central Florida.

Lead Ethical and Sustainable Practices in Your Extended Enterprise

Trust the leader who has partnered with the world's most forward-thinking global brands to operationalize their ESG strategies.

Aravo has the solutions, experience and risk intelligence insights to help you manage and monitor:

- Environmental
- Human Rights
- Diversity
- Ethical Sourcing
- Health and Safety
- Labor Rights
- Supply Chains
- Governance

The Definition of Better Business

Better business is built on acting with integrity.

It commands better performance, delivering better efficiency, collaboration, and financial outcomes.

It inspires trust.

But better business is more than that – it's about lifting the ethical standard of an entire business ecosystem to build a better world.

For More Information

Learn more:
https://aravo.com/products/esg

Email us at info@aravo.com

Call us at:
+1 415-835-7600 [US]
+44 (0) 203-743-3099 [EMEA]

ARAVO