BRC
BOARD RISK COMMITTEE
BOARD RISK REPORT

**August 16, 2021**

# Storm Clouds on the Horizon: Accelerating Challenges in Complex Supply Chain Risk Management

By Bob Jones

In today's world organizational success is most often dependent upon an increasingly large network of external relationships. If we accept the expression that a chain is only as strong as its weakest link, assessing risk in supply chains is impossible when links in the system are invisible. The challenge of managing supply chain risk where unknown 4th, 5th, and Nth parties support critical activities is exactly what risk management professionals face on a daily basis.

This report will discuss four complex supply chain challenges:

- Accurately understanding the length and depth of supply chains and determining appropriate due diligence techniques
- The ramifications of sudden shifts to work-from-anywhere (WFA) environments
- Ethical sourcing challenges in supply chains
- Confronting ransomware in the supply chains

Board members cannot and should not manage the enterprise's supply chain. However, they can be cognizant of and sensitive to the impact that ineffective supply chain management will inevitably have on their enterprise's performance, increasing financial, security, and reputational risks.

The purpose of this report is to provide board members with information they require to ask management more pointed questions about:

- Their organization's identification and prioritization of supply chain risks
- Their organization's ability to confirm that risk management programs are congruent with the enterprise's culture and risk appetite

---

## THE CHALLENGE OF MANAGING NTH PARTIES - HOW FAR DOWN THE SUPPLY CHAIN DO YOU GO?

Third parties are increasingly reliant on subcontractors to help them accomplish their responsibilities to their customers, a cross sectoral trend exacerbated by the use of cloud service providers (CSPs) during the pandemic. That subcontracting can extend far down the supply chain (one financial services regulator referenced 20 suppliers in a single chain, FSB), sometimes without the upstream participants' knowledge. Single points of failure can be managed through the application of sound due diligence and assessment only if they are identified. The failure to understand the complete structure of complex supply chains can lead to several significant risks:

- **Concentration Risk:** Multiple participants contracting with the same provider increases concentration risk both within firms and across sectors. Updating vendor inventories to include all supply chain participants has become increasingly important.
- **Incomplete Due Diligence:** An incomplete understanding of supply chain complexity can create a wide range of risks because of missed due diligence. Outsourcers should contractually require third parties to report their subcontracting arrangements (including scope of work, rationale for sub outsourcing, etc.) to outsourcers. Contracts can (and should) require third parties to levy the same security requirements downstream. Outsourcers can assemble a comprehensive inventory (register) of vendors, an important first step in identifying, assessing, and managing supply chain risks.
- **Regulatory Coherence:** An additional complication has emerged in the financial services business where regulators hold different expectations about an outsourcer's due diligence obligations in complex supply chain management. A stark example is a recent (November 2020) outreach in which the Basel-based Financial Stability Board noted that "most…authorities expect FIs to retain responsibility, and manage risks relating to the subcontracting of services provided by third parties… which can involve fourth parties, fifth parties and beyond." (FSB, page 24). But in newly issued (March 2021) guidance the Bank of England said quite plainly that it "does not expect firms to directly monitor fourth or fifth parties." (BOE, page 30).

**Questions Boards Should Consider:**

- Does management contractually obligate its organization's third parties to:
  - Report the identity of their third parties' subcontractors and the scope of their work?
  - Perform assessments of those subcontractors and share the results with you?
  - Grant rights to accept or reject any subcontractors?
  - Require their subcontractors to place the same conditions on their sub-contractors, and so on?
- Has management completed a vendor inventory?
  - Does that inventory include fourth, fifth, and Nth parties?
  - How often is the inventory updated?

---

**ESG IN YOUR COMPLEX SUPPLY CHAINS**

ESG is a headline issue around the world. News items appear whenever organizational activities have negative environmental or social effects on stakeholders, often with significant reputational, financial, and - increasingly – regulatory consequences.

The practice of ethical sourcing is inextricably linked to knowledge of the Nth parties in any sourcing relationship. Yet one recent study found that although 46% of firms surveyed had a formally documented ESG program, only 14% comprehensively considered ESG metrics in their supplier analyses (ESG Planning and Performance - OCEG). Many firms are just beginning their ESG journeys and are bewildered by standardized ESG metrics that are still works in progress and due diligence regimes that are incomplete. It's no wonder that so many of these companies are looking for a workable path forward.

Some organizations have found initial success in the adoption of an ESG Code of Conduct, used both internally and with suppliers (for example, see Aurelius Group).These codes are often excerpted from more wide ranging conduct codes used internally, and they function best when they are incorporated into vendor contracts. Suppliers are required to agree in writing to conduct business in accordance with the code and may be asked to certify compliance on a periodic basis. When a third party subcontracts

processes on behalf of an outsourcer, parties down the line are asked to subscribe to the same code of conduct, assuring continuity of practice. Some organizations undertake periodic site visits to confirm that the outsourcer's ethical standards are being met.

ESG Codes of Conduct vary – sometimes significantly - from organization to organization, industry to industry, and country to country. That's okay. Codes can be an extremely efficient way to move forward at a time when ESG metrics are unsettled and there is an increasing stakeholder expectation for progress in ethical sourcing.

Because preventing bribery and corruption is such an important component of an organization's ethical sourcing practices, compliance with the Foreign Corrupt Practices Act (15 U.S.C. §78dd-1), enacted in 1977, which applies broadly to all US-based corporations and their supply partners [1], no matter where they operate, is key.

**Questions Boards Should Consider:**

- Does your organization have a comprehensive set of ESG policies and are they actively socialized within the organization and to your suppliers?
- Does your organization have and abide by an ESG Code of Conduct?
- Does your organization ask suppliers to formally agree to abide by your ESG Code of Conduct?
- Does your organization take steps to ensure supplier code of conduct adherence?

---

**THE CHALLENGE OF ENSURING SECURITY HYGIENE IN HIGHLY DISPERSED SUPPLY CHAIN WORKFORCES**

Pandemic-related logistical and hygiene considerations of a work-from-anywhere (WFA) environment forced organizations in nearly all sectors and at all supply chain levels to meet unprecedented challenges in managing information security and human resources while maintaining appropriate employee privacy.

- **Bring Your Own Devices (BYOD) in Unprotected Environments:** BYOD control issues aren't new. What is new, however, is the proliferation of the types and locations of devices brought into the work environment, including routers connected to home networks of phones, tablets, smart speakers responding to voice prompts; and the plethora of Internet of Things (IoT) devices managing appliances, security cameras, etc., common in "smart" homes. Computers used for work may be used for personal purposes in spaces shared by other family members.
- **Invisible Subcontractors:** Work From Anywhere challenges may be harder to detect in subcontractors towards the end of a supply chain, and risks are magnified if the outsourcer either doesn't know they exist or does not adequately understand the environment in which those risks lie.
- **Protecting Your Crown Jewels:** Management has an obligation to protect the organization's sensitive information by monitoring WFA environments, not just internally, but throughout its critical supply chains. At the same time, organizations are obligated to protect employee privacy, and achieving both goals simultaneously produces friction.

**Questions Boards Should Consider:**

- Does your management understand which suppliers (including subcontractors) are being most impacted by their newly dispersed workforces?
- Has management taken appropriate steps to mitigate any disruptions exacerbated by newly dispersed workforces, including protecting IP assets?
- What has management learned about anticipating the possibility of short-term dispersed workforce environments in supply chains moving forward?

---

**THE CHALLENGE OF RANSOMWARE**

While most press reports focus on single victim attacks, ransomware can (and does) play havoc with supply chains. Many organizations are not equipped to deal with a downstream provider who, when attacked, is unable or unwilling to pay a ransom.

On July 3, 2021, Kaseya reported that its servers, which provide central authentication and authorization services for Windows-based computers, had been successfully attacked, taking down the servers of its customers. These customers include managed service providers (MSP's) that provide IT infrastructure services to their customers.

According to Kaseya, 60 of its direct customers and approximately 1500 of their customers, many of which had probably never heard of Kaseya, were affected. The impact included network-connected devices, including point-of-sale networks. The attackers demanded a $70 million ransom for the decryption key. Kaseya stated it had refused to pay. One full week later, on July 12th, Kaseya's networks were largely restored.

Approving a ransomware response policy is probably among the thorniest challenges a board will be asked to address.

**Questions Boards Should Consider:**

- Is your organization prepared to respond to ransomware attacks?
  - Should your organization adopt a strict pay or no pay policy? Should your organization step in on behalf of a supplier if it cannot pay a ransom?
  - Does your organization's cybersecurity insurance policy include ransomware coverage? Does your organization require suppliers to have cybersecurity insurance including ransomware coverage?
  - How does your organization and firms in your supply chain resolve the friction between "official" government policy and the need to restore timely service to your customers?
  - How does your organization deal with a critical downstream provider financially unable or unwilling to pay a ransom?
  - What tactics is your management taking to diminish the impact of ransomware attacks?

---

[1] The Act applies to all US - based corporations, their foreign subsidiaries, foreign companies with US subsidiaries or do business in the US, any company having transactions going through the US banking system, and any US or foreign citizen working for any of those entities.

## ABOUT THE AUTHOR

**Bob Jones, Senior Advisor, Shared Assessments**
Bob has 50 years of experience leading fraud risk management and risk management strategy programs. At Shared Assessments Bob facilitates the Best Practices Awareness Group and UK/EU TPRM Strategies Group. Both have a current focus on supply chain risk management. Bob is Adjunct Professor Emeritus of Economic Crime at Utica College. His articles have appeared in the RMA Journal and the Journal of Economic Crime Management.
Contact: Bob@santa-fe-group.com

## WHO WE ARE

The Board Risk Committee (BRC) is a non-competitive thought leadership peer forum dedicated to Board Risk Committee members and Chief Risk Officers (CROs). The BRC is a trusted place for the exchange of ideas, best practices, and topics of interest. BRC is affiliated with The Santa Fe Group (SFG). SFG is a strategic advisory company providing unparalleled expertise to leading financial institutions, healthcare payers and providers, law firms, educational institutions, retailers, utilities, and other critical infrastructure organizations.

BRC
BOARD RISK COMMITTEE
BOARD RISK REPORT

**March 23, 2021**

# PERSPECTIVES ON BOARD RISK COMMITTEE EFFECTIVENESS FROM A CURRENT AUDIT COMMITTEE CHAIR

In this month's Risk Report we've interviewed long-time Synovus Financial Corporation Board member Joseph Prochaska, Jr. Joe is currently Chair of the Synovus Audit Committee and was founding Chair of the firm's Risk Committee, on which he still serves.

---

***Board risk committees, especially in the financial services sector, have operated for more than a decade. Have they fulfilled their promise? How can risk committees further enhance their value to ensure optimal risk management oversight?***

I believe risk committees have fulfilled their promise. Risk Committees provide an informed, outside perspective of management's actions and efforts around the risks facing their organizations. They also challenge management about how effectively those risks are being managed. helping to identify areas needing improvement and additional focus and highlight areas of organizational strength that can be leveraged. And these committees can help management identify the criteria to critique their enterprise risk management (ERM) program.

It's important to understand that while Risk Committees do not own every risk overseen by a board, the Risk Committee should ensure that all risks are taken into account regardless of risks that naturally reside in different board committees. Well-functioning Risk Committees help the entire Board by assisting in ensuring that all major risks are catalogued and that there is a clear delineation of who within an organization owns each risk and who provides risk management. Risk committees can also help the board feel confident that all identified risks are being overseen from the proper board committee. The risk grid (illustrated below) shows how a generic financial services company may allocate different risks.

Risk Committees routinely focus on emerging risks and ensure that organizations maintain appropriate risk apertures. This "horizon scanning" process has added material value to governing boards by bringing appropriate focus to the full range of emerging risks and ensuring that those risks are properly socialized both on boards and within management. In that way, they have relieved the full board of some of the related burdens, while providing a broader perspective on how the company's risk management can help inform strategic planning and execution.

**Questions for board members:**

- Does management and the Board have a process for periodically surveying for emerging risks?
- Is this list of emerging risks synthesized into an active, prioritized document?
- Does management then work the list and inform the Board of their direction, concern, or action on these items?
- Does the Board provide feedback, not just on the list, but on their priority and on managements' actions related to them?

---

***How have you viewed the relationship between risk and audit committees on the boards on which you've served? How can those relationships be optimized?***

Traditionally the word "risk" was incorporated into audit committee charters, which were primarily concerned with financial risks and focused on past performance, GAAP conformance, and regulatory compliance.

Risk Committees, by design, are forward thinking, examining what could happen and how, when risks occur, and how those risks can be most effectively mitigated. These committees encourage and may participate in regular scenario testing (for example, through tabletop exercises) to help the organization document that plans for material disruption recovery are complete and viable.

I believe risk and audit committees function best when cross-pollination occurs through sharing members and/or chairs across committees. Participation by the audit committee, as well as the whole Board annually, in challenging the risk grid is helpful. It forces everyone to think and challenge the status quo. Joint meetings can be held when topics of interest intersect and outside resources may be used to counsel, coach and/inform both committees.

**Questions for board members:**

- How effectively have risk and audit committees functioned in their complementary roles?
- How often does your board update its risk grid, or equivalent device?

---

***Some boards have structured committees to focus on a particular set of issues, e.g., technology committees (which among other things may focus on cyber security, AI, etc.) and public responsibility committees (that among other things may oversee ESG activities and ESG risk management). When should boards consider setting up such specialized committees?***

First, let's make a distinction between "specialized" committees versus "special" committees. "Special" committees of the Board are typically not standing committees and are chartered for a single purpose. And when that purpose has been fulfilled these committees usually disband.

Examples might include:

- Investigate a shareholder complaint by neutral Board members.
- Address the concerns or plans raised by an activist investor.
- Oversee the remediation of a major cyber breach where conflicts may be perceived among board members.
- Review a merger/acquisition proposal where some of the Board may be conflicted or, for a designated period of time, extra focus is needed and desired.

"Specialized" committees are ones that address a specific area of concern. These areas should have a focus where extra attention is needed for an extended period of time, even if the committee is not permanent. These can be committees of the Board or, alternatively, a sub-committee of an active committee, such as the risk committee.

Examples include:

- A company may be implementing a new critical information technology (IT) system over a period of years. Although IT may be overseen by the Risk Committee, a specialized sub-committee with more frequent meetings and focused concentration may be warranted.
- For a public company with broad "retail" appeal that has as part of its corporate goals/mission to give back and to act for the overall good – a Public Responsibility committee may be warranted.
- A company that has suffered a material cyber breach may need an extended effort to overhaul its cyber management oversight. This could be a stand-alone committee or a sub committee of the assigned cyber oversight committee, such as a risk committee.

**Questions for boards to consider:**

- Does your board have a set of issues that requires a special, prolonged focus that would overtax existing committee structures?
- How can organizations without risk committees judge when establishing such a committee makes sense?
- Many boards have had pandemic disruptions in their risk profiles for years:
- To what extent has planning for severe pandemic disruptions been adequate in our COVID-19 environment?
- Were cascading risks routinely considered such as pandemic plus wildfires or unusually severe storms?
- What could have been done differently to improve outcomes?

## ABOUT THE AUTHOR

Joseph J. Prochaska, Jr. is the retired Executive Vice President and Chief Accounting Officer of MetLife, Inc. Joe is currently the Chair of the Audit Committee at Synovus Financial Corporation. In 2011 Joe stood up Synovus' first Board Risk Committee on which he still serves and which he chaired for several years. In 2018 he was named to National Association of Corporate Directors (NACD) Directorship 100, which "honors board members who serve as role models in promoting exemplary board leadership and courage in the board room." Joe serves on the Board of Directors of the Santa Fe Group."

## WHO WE ARE

The Board Risk Committee (BRC) is a non-competitive thought leadership peer forum dedicated to Board Risk Committee members and Chief Risk Officers (CROs). The BRC is a trusted place for the exchange of ideas, best practices, and topics of interest. BRC is affiliated with The Santa Fe Group (SFG). SFG is a strategic advisory company providing unparalleled expertise to leading financial institutions, healthcare payers and providers, law firms, educational institutions, retailers, utilities, and other critical infrastructure organizations.

BRC
BOARD RISK COMMITTEE
BOARD RISK REPORT

**January 15, 2021**

# 2021: ESG ASCENDS IN AN EVOLVING RISK LANDSCAPE

**By Catherine Allen and Gary Roboff**

Environmental, social, and governance (ESG) concerns will be a top priority for boards in 2021 and beyond. Boards will be increasingly focused on environmental, diversity, social responsibility, resource sustainability, appropriate governance, and other ESG issues. However, the United States lags other regions in its attention to ESG issues and too often both boards and investors do not see an economic advantage in pursuing them. A recent Royal Bank of Canada (RBC) Global Asset Management Responsible Investment Survey found that just 65% of firms in the United States view ESG issues as important in investment strategy and decision-making, versus 94% in Europe and 89% in Canada. Frustrated Exxon-Mobil shareholders are mounting a significant effort to oust a set of board directors because of an ongoing lack of attention to ESG issues. The unfortunate reality is that too many boards are not structured to optimally consider ESG issues and understand the benefits that would come from addressing their impact.

## WHY IS ESG OVERSIGHT SO IMPORTANT TO BOARDS?

Increasingly, boards recognize that the right ESG policies can generate significant economic value. Boards also recognize that failure to appropriately manage risks arising from ESG issues can lead to reputational issues, government regulation and enforcement actions, private litigation, and an increasingly negative impact on shareholder value. Adoption of ESG principles is growing globally, according to the recent 2020 RBC Survey. Overall, more than 75% of the respondents integrate ESG principles into their investment approach and decision-making. The pandemic has required boards and investors to pay greater attention to supply chain risks and a host of ESG issues, including workplace culture and safety. Investor advisory groups, such as Glass-Lewis and ISS, and large Investors, such as BlackRock (an ESG leader) and State Street Global Advisors, are increasingly emphasizing ESG in corporate proxy disclosures and director elections materials. These firms understand the consequences of climate change, are uneasyabout social unrest, and acknowledge the increased scrutiny coming from regulators.

ESG is a priority on advisory firms' suggested 2021 board agenda items. For example, KPMG's Board Leadership Center's 2021 Board Agenda identifies COVID-19, human capital management and CEO succession, combating systemic bias and racism, refocusing on ESG, and crisis readiness and resilience asits top five focus areas.

A recent Pew Research Survey shows 9 of 10 consumers believe corporations should be accountable for more than profit. Younger generations such as Millennials and Generation Z want to work for companies that align with their personal missions and those cohort groups look at how companies are handling issues such as climate change and diversity and inclusion. To attract and retain talent now and in the future, boards need to understand the demographic changes that are driving attention to ESG.

**What Can Boards Do?**

- Talk to your investor relations executives as well as your investors about what your organization's strategy is around ESG.
- Have regular discussions at the board level on ESG.
- Make sure your proxy statements have appropriate information about board oversight and disclosure of issues.

---

## HOW ARE REGULATORS IN THE US AND ABROAD LOOKING AT ESG?

Regulators are paying increasing attention to ESG risk issues, but until now not always with consistent direction. President-Elect Biden, however, has made environmental and social issues a key part of his policy agenda.

At a global level, the Financial Stability Board's (FSB's) Task Force on Climate-related Financial Disclosures has issued a consulting paper on Forward-Looking Financial Sector Metrics (comments accepted through January 27th). The European Banking Authority has an open consultation on an approach to incorporate ESG risks into the governance, risk management and supervision of financial services companies (comments accepted through February 3rd). In early December, the U.S. Securities and Exchange Commission's Asset Management Advisory Committee issued preliminary recommendations that would require the adoption of standards through which corporate issuers would disclose material ESG risks.

Boards should anticipate that ESG disclosure requirements (and eventually compliance responsibilities) will apply broadly and will extend to organizational supply chains, including mandatory requirements for vendor disclosures as part of periodic third party risk management due diligence.

**What Can Boards Do?**

- Make sure your organization examines current, and draft, ESG regulations to understand and comment upon regulatory direction.
- Encourage management to review your organization's ESG risk management strategy with regulators and to explain its thinking about particularly important ESG elements.
- Ensure your organization will be able to comply with ESG regulations as they are released.

---

## ESG METRICS: THE ESSENTIAL - BUT NOT QUITE READY FOR PRIME TIME - RISK MEASUREMENT TOOL

It is difficult for any organization to know whether it is managing ESG risks effectively without a set of widely accepted ESG metrics in place. In recent introductory language to rules limiting investment advisors' ability to incorporate ESG considerations into some retirement portfolios, the "EBSA concluded that the lack of a precise or generally accepted definition of 'ESG,' either collectively or separately as 'E, S, and G,' made ESG terminology not appropriate as a regulatory standard." Others have recognized the issue and are attempting to address it.

One important effort, led by the World Economic Forum (WEF), issued suggestions last September. WEF's proposed cross-sector metrics, designed to work across all industries, were based on five key criteria:
-consistency with existing frameworks and standards
-materiality to long-term value creation
-extent of actionability
-universality across industries and business models
-monitoring feasibility of reporting

We believe a two-tier set of metrics will eventually emerge – first, a smaller set of ESG metrics that are appropriate to organizations across all sectors; and second, sets of industry-specific ESG metrics.

**What Can Boards Do?**

- Make sure your organization is paying close attention to emerging ESG Metrics.
- Be sure that your organization offers carefully considered perspectives when regulators are requesting feedback on proposed ESG metrics (many are).
- Establish and track progress to achieving a clear set of ESG organizational goals.
- Ensure your organization will be able to comply with ESG regulations as they are released.

---

## HOW ARE BOARDS ADDRESSING ESG ISSUES FROM A GOVERNANCE AND STRUCTURAL PERSPECTIVE?

Many boards are approaching ESG discussions either at the full board level or parsing issues to various committees, including:
-Audit or risk committees to oversee ESG related risks,
-Compensation committees to ensure diversity and inclusion,
-Corporate governance committees often to add a responsibility for overseeing sustainability issues,
-Public responsibility committees which oversee matters such as sustainability and other public policy issues that reflect organizational character and can impact reputation among all stakeholders.

Board risk committees can bring unique value-add when overseeing ESG related risks because they can best place those risks within an organization's overall risk framework. That is important because one group of risks will likely impact others and overseeing any set of risks in a vacuum may create a sometimes strikingly incomplete picture of the risks actually facing an organization.

**What Can Boards Do?**

- Ensure that ESG oversight responsibilities are distributed to committees with appropriate expertise.
- Recruit ESG talent to the boards and establish regular full board ESG briefings, at least on a quarterly basis.
- Review your organization's ESG policies, strategies, and risk appetite on a regular basis.
- Update the organization's risk profile to include all issues related to ESG.
- Invite outside experts to brief the board on such issues as climate change, diversity (including board diversity) and inclusion, and social unrest.

## RESOURCES

Royal Bank of Canada (RBC) ESG Executive Summary

KPMG: On the 2021 Board Agenda

TaskForce On Climate-related Financial Disclosures - Consultation and Input

EBA Consultation to Incorporate ESG Risks Into Governance, Risk Management and Supervision of Credit Institutions and Investment Firms

U.S. Securities and Exchange Commission Asset Management Advisory Committee Potential Recommendations of ESG Subcommittee

Final Rule on Financial Factors in Selecting Plan Investments

Measuring Stakeholder Capitalism Towards Common Metrics and Consistent Reporting of Sustainable Value Creation

10 Ways Corporate Boards Need to Approach Risk in 2021

C-Suite Call to Action – Risk Management Through A Different Lens

*"ESG is real, it took off a while ago, it's going to continue to grow…. It needs to be done maturely and intelligently."*

**Jamie Dimon**
Chairman and CEO
JP Morgan Chase & Company

## ABOUT THE AUTHORS

**Catherine Allen** is Founder and Chairman of The Santa Fe Group and a corporate board director for privately held and family businesses. She formerly served on the public corporate boards of NBS Technologies, Stewart Information Services, Synovus Financial and El Paso Electric Company. She has created, chaired and sat on numerous Board Risk Committees. She was named one of the NACD Most Influential Directors in 2018 and sits on the Advisory Board of Women Corporate Directors.

**Gary Roboff** is Senior Advisor to The Santa Fe Group and a former financial services executive at J.P. Morgan Chase. Gary has served on the Board of Directors at multiple companies and organizations including ISTPA, the NYCE network, and the Electronic Funds Transfer Association. Gary served on the Board of Trustees at Clark University for 12 years, nine of them as Board Vice Chair and as Chair of the Board's Strategic and Financial Oversight Committee.

## WHO WE ARE

The Board Risk Committee (BRC) is a non-competitive thought leadership peer forum dedicated to Board Risk Committee members and Chief Risk Officers (CROs). The BRC is a trusted place for the exchange of ideas, best practices, and topics of interest. BRC is affiliated with The Santa Fe Group (SFG). SFG is a strategic advisory company providing unparalleled expertise to leading financial institutions, healthcare payers and providers, law firms, educational institutions, retailers, utilities, and other critical infrastructure organizations.

**CONNECT WITH US**

BRC

BOARD RISK COMMITTEE

# BOARD RISK REPORT

September 15, 2020

## A FUNDAMENTALLY CHANGED RISK ENVIRONMENT

There is no "returning to normal" in the future…the new normal will be continuous change and boards will face an increasing need to make decisions in the face of uncertainty. To properly understand the range of COVID-19 outcomes that will shape the economic and logistical environments during the next 18 months and beyond it is essential that enhanced horizon risk scanning and techniques such as scenario planning and modeling are utilized. These techniques will help firms make decisions about the impact of the virus environment, which will continue until there are enough tests, a vaccine, and a reliable way toimplement contact tracing. That may take more than 18 months and, because of infection cycles, there may be a new virus that emerges by then.

**What boards should do:**

- Ask management what risk modeling and scenario planning tools they are using to help predict economic and business interruptions.
- Set board (and enterprise) expectations that increased levels of uncertainty will continue and develop enhanced horizon scanning techniques that are sensitive to a broader range of risks.
- Make sure geopolitical and environmental risks are appropriately considered.

---

## CHIEF RISK OFFICERS AND RISK COMMITTEES OF THE BOARD ARE IN DEMAND

In addition to Succession Planning, Strategy and Fiduciary Responsibility, Risk Oversight is becoming the fourth key responsibility of boards. Today's rapidly changing risk environment (led by COVID-19, environmental catastrophes and political uncertainties) has put a spotlight on the criticality of an effective enterprise risk management program. Boards with both Chief Risk Officers (CROs) and Risk Committees are leading the charge in actively managing risks. Where optimum board risk oversight capabilities are not already present, demand for CROs and Risk Committees has escalated.

**What boards should do:**

- Create risk committees, at both management and board levels, including directors and executives with risk, cyber, operations, communications, and technology backgrounds.
- Create the position of Chief Risk Officer (CRO), reporting to the CEO, with dotted line reporting to the Chair of the board's Risk Committee.
- Include Risk Committee discussions of emerging risks on board meetings at least quarterly.
- In situations where an organization is actively building or enhancing an enterprise risk management program, boards should monitor progress regularly.

SOURCES: WOMEN CORPORATE DIRECTORS, NACD

## TONE AT THE TOP - CRITICAL IN HOW COMPANIES TREAT STAKEHOLDERS DURING PANDEMIC AND ECONOMIC DOWNTURN

Organizations that are sensitive to stakeholder needs will benefit through enhanced abilities to attract and retain talent and will build stronger vendor relationships. The COVID-19 crisis will create lasting memories - stakeholders will remember where they were, what happened, and how they were treated...either with compassion and integrity, or not. Everyone in the current environment has been affected, many by illness, loss of income or revenues, and by adapting to a new way of work. Companies that appropriately engage with their employees and vendors to optimize outcomes for all will generate greater respect and loyalty that will pay dividends in the future.

**What boards should do:**

- Oversee management activities in support of all stakeholders, including employees and vendor relationships, and ensure that expectations are being met.
- Include Talent Management personnel at board meetings to report on how employee related initiatives are being created, monitored, and received.
- Add a Talent Management professional to the board of directors if appropriate expertise is not already in place.
- Expand the Compensation Committee to include a broader Talent Management and culture of responsibility.

SOURCE: WOMEN CORPORATE DIRECTORS COMMISSION ON TALENT MANAGEMENT REPORT: WORK HAS CHANGED

## EMERGING RISKS OF IoT, THE INTERNET OF THINGS

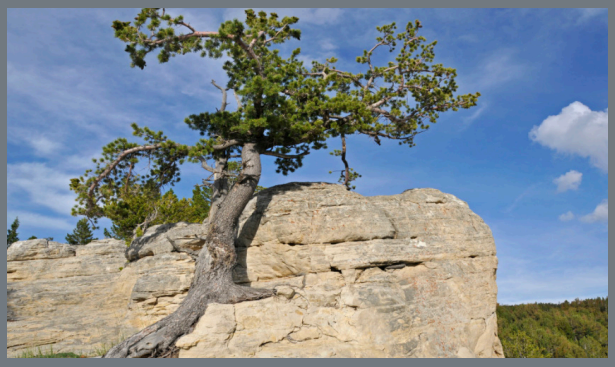
Recent studies show that most organizations do not have adequate knowledge about the number and type of IoT devices connected to their networks, do not adequately secure them, and do not have an effective IoT risk management program. The consequences of ineffective IoT risk management programs have been magnified because of COVID mandated work from home environments, which seem likely to continue in some form. Home IoT devices include smart phones, tablets, printers, televisions, kitchen appliances and other electronic equipment. Improperly secured home networks utilizing sub-optimally secured work from home equipment increase already substantial IoT risks. As the number of improperly secured IoT devices proliferates, the risks to organizations increase.

**What boards should do:**

- Ensure an effective IoT risk management program with clearly defined responsibilities is in place.
- Ask management for an inventory of IoT devices connected to company networks and ask how that inventory is updated.
- Ask management what work from home security policies and protocols are in place and how those protocols are enforced.
- If the board does not fully understand IoT security risks, bring in experts for a board/risk
- committee briefing.

SFG | Shared Assessments Ponemon Research on IoT

SOURCE: SFG | SHARED ASSESSMENTS PONEMON RESEARCH ON IoT



*"Strength does not come from physical capacity. It comes from an indomitable will."*

Mahatma Gandhi

## UPCOMING EVENTS

### The Need For Board Risk Committees: Part 2


Women Corporate Directors and The Santa Fe Group are partnering for a WCDirect Zoom event, "The Need for Board Risk Committees: Part 2." During this session, panelists will address emerging operational risks, the value of Board Risk Committees, and what it takes to form one and follow best practices.

September 29, 2020
2:00 p.m. – 3:30 p.m. (U.S. EDT)

Register To Attend

## WHO WE ARE

The Board Risk Committee (BRC) is a non-competitive thought leadership peer forum dedicated to Board Risk Committee members and Chief Risk Officers (CROs). The BRC is a trusted place for the exchange of ideas, best practices, and topics of interest. BRC is affiliated with The Santa Fe Group (SFG). SFG is a strategic advisory company providing unparalleled expertise to leading financial institutions, healthcare payers and providers, law firms, educational institutions, retailers, utilities, and other critical infrastructure organizations.

**CONNECT WITH US**