Threat Management

Evolving perspectives amidst the pandemic

by Maurice Evlyn-Bufton, CEO of Armstrong Wolfe
March 2021

ARMSTRONG WOLFE

Defining Threat Management

Entering 'threat management' in the Cambridge Dictionary it will offer you 10 disciplines of management: talent, event, asset, time being four, but threat is not one of them. As an alternative it presents: You can also search for 'threat' and 'management'.

- **Threat:** a suggestion that something unpleasant or violent will happen, especially if a particular action or order is not followed.
- **Management:** the control and organisation of something

(Cambridge Dictionary)

If you complement this with a Google search using 'threat management definition' as your reference, you are taken to a multitude of options and opinions. All, however, see threat management as an umbrella term for the computer security and information security programmes instituted in an organisation. Clearly the concept of holistic threat management has not become common practice. Why is this?

There is a point of view that threat and its many dimensions, come together at the intersection of non-financial, conduct, cyber, ESG, geo-political and enterprise-wide risk. These established risks have become increasingly overshadowed by climate change, which poses significant risks to the financial system, particularly for the insurance and banking sectors. The question is whether a clustering of this data could be generated allowing value assessments to be made in a broader threat management context?

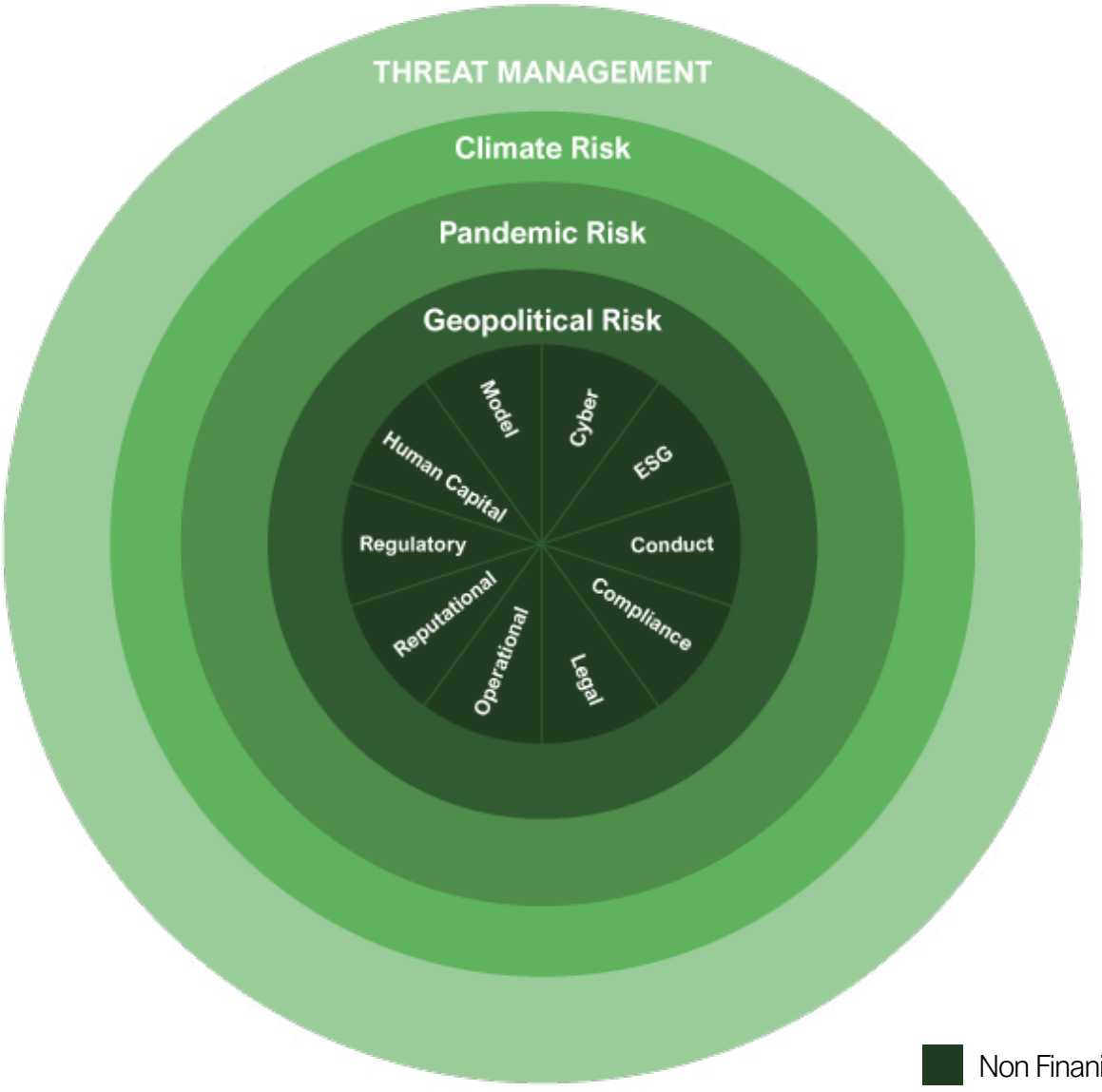
Additionally, Covid-19 re-emphasised the importance of pandemic risk management. The short-term risks and challenges presented to employers include an unforeseen change in working practices, with industry workers proving they can be just as productive and accountable when WFH. How the industry and its participants will deal with this change in the long-term is to be determined. The importance of getting your positioning right, however, and investing in precise training, tooling, and rewarding of staff (to maximise workforce performance in the new world post pandemic) could materialise into a human capital risk. This risk is important within an industry highly reliant on hiring and retaining the best people, and where workplace options may shift the focus from corporate allegiance and compensation to work placement optionality and culture.

Human Capital Risk in this context is heightened when additionally accounting for the evolving liabilities on mental health and a duty of care towards employees and more materially, the anticipated conduct and cultural challenges that will become evident with the passage of time.

Threat, you could argue, is uttermost when one meets another or triggers another. More so, in the case of the pandemic and like the disease itself, its consequences are contagious, fuelling other risks to become an exponential one.

Threat Management could therefore be defined as is a discipline that is complementary to and encompasses established risks and is best understood in the capacity of horizon scanning and the ability to detect and determine actions to emerging risks. Its methodology would rely on the integration of established risk data, to be looked at in real-time with its aim being to detect early signs of potentially important developments (that could impact the business) through a systematic examination of potential threats and opportunities, with an emphasis on the use of new technologies, data aggregation and digitisation.

Non-Financial Risk within the continuum of Threat Management



Post Pandemic

An opportunity to change thought and action for the COO?

The pandemic is an interesting case study to apply thought for holistic threat management. All the threats listed above have been surpassed and to differing degrees, stimulated by a lack of pandemic risk management. We have an established understanding that a pandemic is a rapidly spreading infectious disease that may (SARS 2002 and 2004) and could (Covid-19) show a pandemic's ability to create social and economic chaos, severely upsetting business operations and producing disruption in the supply chain. It has further impeded commerce and industry's ability to deliver products and services to customers.

Unquestionably, therefore, managing the threat posed by a pandemic is critical for business survival.

To do so we must ask, what is the international community's and individual nation's risk appetite and risk tolerance [in the context of a pandemic]? How much risk management is enough? What are the responsibilities of corporations as well the regulators that monitor them? What expectations should customers have and what liability should banks, asset managers and financial institutions accept in managing this risk? Without addressing these and similar questions, we are likely to end up with poorly conceived, contradictory, and costly strategies that could increase risk.

Policy making is part of the solution, preparedness another, but horizon scanning and looking at this challenge through a forward-looking, threat management lens, could make a material difference to a business and/or the industry's ability to anticipate such events and mitigate damage (when it next happens).

This risk must not be looked at in isolation. Where post-pandemic reviews will point to failures of governments to prepare and meet their obligations and industry-wide failures to prepare for such an inevitability will also be identified. These failures and lack of preparedness will be better handled in the future if managed as an inevitability, a threat that will materialise, and if planning to meet this inevitability is mandatory. It is a matter of 'when' and not 'if'. If this assumption is accepted, there will be a need to place its influence and impact in a perspective of understanding how it could promote, effect and shape other risks and events.

So what? This question arises when a threat or series of apparently unrelated threats arise at the same time. Who in any company is positioned to guide the CEO and to help set an anticipatory course of action based upon a broader appreciation and understanding of threat management? Presently such guidance is not supported by an aggregated data of all risks and is given in respective quotas by the CRO, the CISO, Legal, Compliance and the COO. What a different approach to threat management could enable the CEO to do is make decisions in confidence and to the best of his/her knowledge and abilities (based upon a uniformed assessment of all risks).

Creativity within Threat Management

The commercial consequences of the pandemic were made worse by the industry having no meaningful pandemic risk management system in place. More so, it was a failure of the imagination. This threat has existed throughout modern mankind's 100,000-year residency on Earth; pandemics having a routine visitation on humanity. Many refer to the Spanish Flu pandemic (1918-1920), although there were three worldwide pandemics and outbreaks of influenza in the 20th century: 1918, 1957, and 1968. The latter two were in the era of modern virology and most thoroughly characterised. All three have been informally identified by their presumed sites of origin as Spanish, Asian and Hong Kong influenza, respectively. Recently there were two self-limiting SARS outbreaks in 2002 and 2004. The limitation and containment of their impact may in part explain the lack of preparedness for Covid-19. It is clear post SARS incomplete contingency planning was adopted to meet a future pandemic. This has prompted reviews of how Covid-19 should have been an anticipated event. In doing so policies should have been developed within contingency planning to meet this challenge.

Lessons learnt? What is important is the role of creativity and open thought, the active promotion of asking the 'what if', and the right to suggest and assess the improbable becoming possible.

"Not thinking it's possible is a failure of the imagination"

- Vinod Khosla

(co-founder of Sun Microsystems)

Is there a role for the COO within Threat Management?

In line with pre-pandemic thoughts on threat management and responding to feedback from the COO community attending our forums amidst Covid-19, we undertook a market survey and set a series of COO cluster calls to discuss the possible benefits and challenges of managing threat holistically.

Some COOs had highlighted an evolving expectation, to have an appreciation, to understand real time operational and non- financial risk, but in a broader context. They were being asked to do so with a fragmented and disconnected view of the overall threat and risk landscape.

Questions arising from these cluster calls set the survey:

- How the COO can establish a better view and understanding of the threat and risk landscape, and what challenges do they foresee?
- How to differentiate between the responsibilities of the COO, CRO and Heads of Legal.
- Compliance, to define a new approach to managing risk and threat that works in the best interests of the organisation.
- What are the areas of support and improvement the COO is seeking in this context to enable them to deliver on their principal responsibility – to protect the franchise.

In conducting the review, Armstrong Wolfe surveyed a representation of COOs from across the community, buy and sell side. The survey was broad in nature, and sought opinions on:

- A view on the maturity and effectiveness of the risk management framework.
- The focus in risk meetings & the extent to which it is “here and now” versus horizon scanning.
- The engagement across the c-suite, particularly with CRO, CISO, legal & compliance.
- The use of risk information within the firm, and the confidence in the quality of data analysis.
- A view on risk systems and process and what they believe could be improved upon.

Survey Output

a. Proactive Identification of Emerging Threat

COOs were unanimous in the view that for their role to be most impactful, they require a broader and more informed view across risks and threats which impact the franchise. They see the ownership and stewardship of risk as a collective responsibility and are well positioned to support in the translation of those risks into deliverable action plans. There is a challenge, in that the prevalent use of people's time and the focus in risk meetings is on the "here and now". Some firms have invested energy into considering emerging trends and horizon scanning, though this practice could be more robust and where it is conducted is focused more to regulatory change, or cyber, with less consideration given to geo-political events.

b. Efficient Governance Structure with Global Reach

COOs do not see the potential for conflict with the CRO, CISO, legal and compliance, if they were to have a broader view across threats and non-financial risks. There was a consistent message that they must work proactively to make those relationships effective, and to ensure those functions fully understand a local or regional concern and the potential business impact of it. While COOs value the independence and challenge from those roles, there can be issues where there is a strong vertical reporting line for those functions. COOs are looking for the governance structure to enable a more holistic and informed view of the overall risk landscape so they can fully consider its implications.

c. Enable Strategic Decision Making & Operational Control Implementation

Over 70% of survey respondents were not fully aware of the breadth and depth of risk information available within the firm, did not fully understand how it was collated, analysed and distributed, did not believe it was presented in a digestible format and did not have full confidence in it, nor the analysis that accompanied it.

Risk data and metrics can be very granular, which can be helpful at one level, but can make it harder to identify the material issues quickly. The information packs for risk meetings are often too large, with concerns expressed about the ability to digest them fully beforehand. As it can take time to get to the heart of the real issues, a consequence is that there can be insufficient time spent considering emerging risks and to conduct horizon scanning.

d. Prioritises Leveraging Internal Resources to Focus on Highest Risk Issues

To address this challenge, while there is some trade-offs that can be made by COOs, including delegation of activities to declutter their inbox, there was a clear message that they see the need to attack the problem of prioritisation with improvements in data and automation.

e. Leverage Technology

When asked to consider how effective risk management was in the context of strategy, governance, culture, business, and operating models and against the use of data & technology, the weakest area by a clear majority was on the use of data and technology. Examples provided included continued use of legacy systems, underinvestment in technology and the ongoing reliance on Excel. COOs want better structure and organisation of the data, particularly regarding the mapping of data into risks to further aid the analysis to enable them to get to the more material issues quickly which will free up time to consider emerging trends and conduct horizon scanning.

2. Bearing in mind this feedback, working with a risk management 3rd party, we sought to demonstrate the range of solutions that could be brought to bear to support COOs across a range of issues of varying scale and complexity. At one end of the spectrum were specific insights into a proven ability to analyse and advise on a specific geo-politically driven event and its ability to severely impact a financial services organisation, namely the imposition of the new Hong Kong national security law. This included:

- **Concerns as to how MNCs might have to flex and structure themselves to** handle an increasingly adversarial sovereign relationship between China and the USA.
- **Determining how well banks in turn understood how their clients** in Hong Kong specifically and Asia generally might be reacting to this worsening relationship.

- **The impact on Hong Kong's reputation** as a place to live and work for professional expats and HK residents.
- **The potential alternatives** to Hong Kong should institutions be forced to relocate in the region, and the risks associated with those options.
- **Impact on back office operations** – For example there has been talk of the US using the threat to cut China off from the global SWIFT messaging and payment settlement platform. While China has its own internal clearing system, it does not yet have the same adoption. If it were to scale up, what does that mean for back office processes, or data security, and for ensuring systems and operations integration to execute seamless processing, transaction monitoring and screening?

3. At the other end of the spectrum, we outlined experiences of designing and helping clients implement programmatic solutions which explored how institutions tackled the challenge of collating, analysing and disseminating non-financial threat and risk data in a manner which addressed the issues COOs were most concerned about in the survey feedback.

The overarching principles of such programmes can best be summarised below:

MUST:

- Identify high risk scenarios according to rigorous and consistent criteria.
- Inform decisions and controls with risk-focused intelligence assessments.
- Connect dots between siloed analytics and intelligence.
- Focus on proactive indicators and early warnings.
- Involve liaison with other teams on assessment methodologies.
- Conduct targeted multi-source data analytics.

MUST NOT:

- Own risk, but rather be a force multiplier to help lines of business manage their own risk.
- Duplicate or usurp risk-management efforts by other units already under way.
- Overestimate its ability to predict events or influence outcomes.
- Infringe on privacy regulation, national or international law, or adversely impact corporate culture.
- Rely on dragnet analytics or experimental technology instead of human capability.
- Over-spend before establishing a consistent and proven initial capability.

We also discussed the different delivery models that could be used to deliver such a programme, the roadmap involved and example projects, timelines and indicative costs.

4. What do we seek to understand from you?

a. Does the feedback from the survey resonate with you? If so, how specifically does it impact you in your role?

b. Are you motivated to make change at your organisation and if so, what is the strength of your current interest levels and ability to effect that change?

c. What help do you need to scope the requirement and/or communicate the need internally if any?

By way of guidance re: the above, and from our two workshops with the Markets and Asset Management COO communities, the feedback on this set of questions was:

- Two global brands felt they wanted immediate support with geo-political horizon scanning beginning with China and the trajectory of the future relationship with the USA, and secondly, clarity around the scenarios relating to Hong Kong and the impact of the national security law on their HK operations.
- One global brand seeks analysis on the potential for severe market, economic and societal impact in the USA in the event of a closely contested and disputed election.
- One global brand wanted to discuss how to broaden and deepen the array of high-quality data sources and analysis relating to non-financial threat and risk that they were using to inform their strategic decision making (and subsequent operational controls).
- One Asia focused brand wanted to discuss a full programmatic approach to non-financial threat and risk management.

Case Study: geo-political risk.

What does this mean for the COO?

The next phase of evaluation of how to (or whether we should) operationalise an approach to threat management, will be to take geo-political risk as a case study, and apply collective thought to its management from a COO's perspective.

We will assume that the top of the house, the board, regularly receives geo-political assessments from one or other of the world's leading advisory firms. The question is how this information is distributed and what analysis is undertaken to answer the question 'so what?' We will investigate how this data could be better used to help the COO take anticipatory actions and take the COO from a reactive, on the back-foot position to one that can initiate actions to dilute the potential impact of this risk. We will also look, through lateral thought and dissection, and speculate how this risk could have unforeseen impacts on different parts of the entirety of the business.

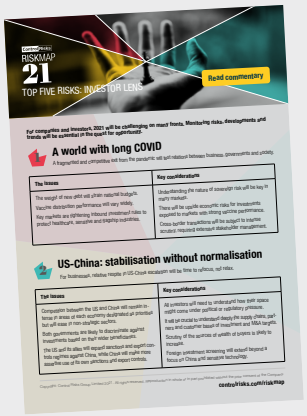
This will be timely, as 2021 – 2022 will be challenging on many fronts for companies and investors. Monitoring risks, developments and trends will be essential in the quest for opportunity; identifying the primary risks and then analysing them through the 'so what' lens will be key to finding a path to progress.

We will present geo-political risk at a series of COO cluster calls, testing the above and debating how the COO (or if not the COO, who?) could play a role in managing threat. Whosoever would need to be armed with the data to interpret and translate into answers and perspectives to the question 'Threat - so what?" Where notedly the inability to provide data is an emerged problem of an imperative nature and as such, a principal threat.

2021 geo-political risks
All change with a New U.S. President + China & Hong Kong + Cyber Warfare + India-Pakistan + Popular Unrest +

More Difficulties for Western Democracy + Gulf Conflict + Technological Arms Race + Latin American Divisions + Protectionism & Isolationism

Read the full article here...



Download

ARMSTRONG WOLFE

CONTACT US

Maurice Evlyn Bufton, CEO
maurice.evlyn-bufton@armstrongwolfe.com

Gwen Wilcox, COO
g.wilcox@armstrongwolfe.com

Find us on LinkedIn: Armstrong Wolfe | Women in the COO Community | Global COO Community