Risk Matters

A SEMI-ANNUAL PUBLICATION | FALL 2019

"The pessimist complains about the wind. The optimist expects it to change. The leader adjusts the sails."

Beyond the Numbers
Five Years of Risk Trends

RC ANSWERS:
What are some emerging trends in risk management?

Featured Risk Leader:
Inga Beale DBE

Risk Cooperative

Contents

"Leadership and learning are indispensable to each other."

Risk Matters

Risk Cooperative
1825 K St. NW, Suite 500
Washington, D.C. 20006

+1 202.688.3560
info@riskcooperative.com

Risk Matters is published semi-annually by Risk Cooperative to move risk from being a cost to becoming a catalyst for change, new initiatives and greater resilience around the world. With this and our latest curated content, we aim to advance the standards of practice of the risk and insurance profession.

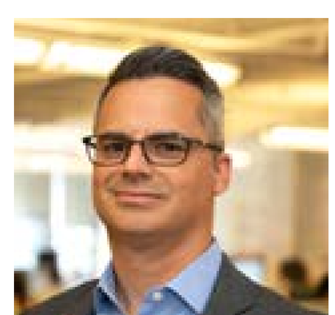
Foreword

This is a very special issue of *Risk Matters*, as it marks the 5-year anniversary of Risk Cooperative. Over the past five years, the global risk landscape has changed significantly. We have seen the emergence of a host of complex and intangible risk domains challenging the fundamental way corporations do business around the globe. Cyber, once a term that would need in-depth explanation to the average American, has now become part of the common lexicon. Natural disasters—record breaking floods, fires, and storms—and greater political instability from world powers require companies of all sizes to rethink how they manage their risks.

When we set out to found Risk Cooperative, it was with this fast-evolving risk landscape in mind, sensing that the risk management and insurance solutions available at the time were not adequate to properly mitigate the threats they must face. The past 5 years have proven this hypothesis correct. We have seen a daily onslaught of cyber breaches, where insurance claims are determined in the courtroom rather than between the insured and the underwriters. We've seen entire communities displaced due to extreme weather events occurring with more frequency and severity. And we've seen the proliferation of technology solutions and connected devices both increase vulnerabilities, while at the same time create opportunities for risk reduction.

In this issue we explore not only at how the risk landscape has changed, but also the new classes of intangible assets that must now be protected. From digital assets, the enterprise value of digitization efforts, and reputational exposures, organizations now need to evaluate a wider scope of values when determining their risk management strategies and appetites. This issue of *Risk Matters* looks at the various ways we can help to prepare for greater operational resiliency. Our work these past five years has allowed us to tackle innovative enterprise risk management strategies and develop programs to address even the most complex risks.

The last five years have taught us that we can no longer manage risk by looking in the rear-view mirror at yesteryears data. By shifting to a more agile risk posture, and aligning risk management with strategic objectives, organizations can create risk agility and resiliency to operate in this new risk world.



Andres Franzetti is the Co-founder and Chief Executive Officer of Risk Cooperative

Featured Risk Leader

Dame Inga Beale is a renowned public speaker, businesswoman, and the former CEO of Lloyd's of London – the iconic 330-year-old insurance and reinsurance market. With over 35 years of global experience in financial services she was awarded her damehood in 2017 for services to the UK economy.

DAME INGA BEALE,
PUBLIC SPEAKER, CONSULTANT AND
FORMER CEO OF LLOYD'S

During her 5 year tenure at Lloyd's, Inga modernized the $40 billion insurance giant through the introduction of technology, moving it from a paper-based market to an electronic trading environment, but without losing "the magic" that makes Lloyd's what it is.

Importantly, she embedded a culture of innovation with the opening of the Lloyd's Innovation Lab in the heart of the market and expanded into new, high-growth markets including China, Dubai, and India.

As the first female CEO of Lloyd's, she also played a critical role in advancing diversity and inclusion initiatives across the global insurance sector including the Dive In Festival, a movement to support the development of inclusive workplace cultures. The festival is now in its fifth year with events in over 60 cities in 30 countries around the world.

Prior to Lloyd's, and from her early days in the 80's as a trainee at the Prudential in London, Inga has lived and worked in France, Germany, Switzerland and the USA, taking on global CEO roles for insurance groups Canopius and Converium, and been in executive leadership roles at large financial institutions such as Zurich Insurance and General Electric's GE Capital.

Inga has served on numerous boards over the years in a non-executive capacity and is currently a member of the London First Board and the London Mayor's Business Advisory Board. She is currently Patron of Insuring Women's Futures, an organization that brings together insurance and personal finance professionals to improve women's lifelong financial resilience. Her philanthropic interests include being an advisor to the LGBT charity Stonewall and the Pitt Rivers Museum at Oxford University. Inga's committment to tackling industry challenges through innovation, and her relentless advocacy of diversity and inclusion initiatives has made an indelible mark on the financial services industry. It is our honor, as we mark Risk Cooperative's 5th anniversary, to name Dame Inga Beale our Risk Matters Featured Risk Leader.

"I thought, I'm really excited about taking this job on, I must modernise this market because it's so special, yet I realised if we didn't introduce technology we would be losing out to the rest of the world. What I didn't realise at the time was the amount of work that needed to be done around the culture."

RISK MATTERS | FALL 2019

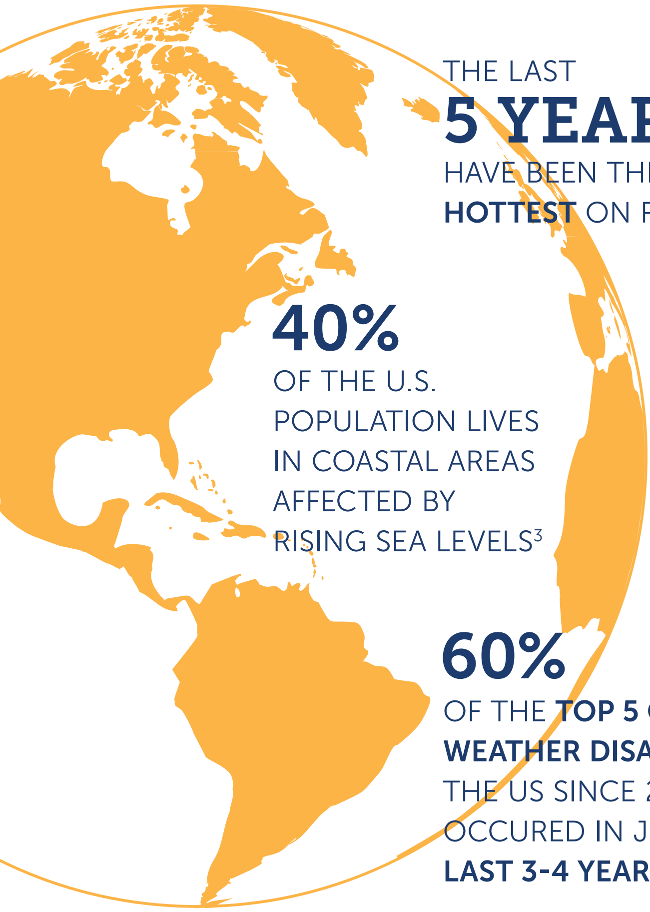
By the Numbers

RISK TRENDS OF THE PAST 5 YEARS

EXTREME WEATHER

Just this week the World Meteorological Organization announced a new record high in atmospheric, heat-trapping greenhouse gas concentrations[1].

The resulting surface temperature changes are fueling extreme weather events that have increased dramatically in frequency and rate since 2014, costing billions and challenging our national security.



THE LAST **5 YEARS** HAVE BEEN THE **HOTTEST** ON RECORD.[2]

40% OF THE U.S. POPULATION LIVES IN COASTAL AREAS AFFECTED BY RISING SEA LEVELS[3]

60% OF THE **TOP 5 COSTLIEST WEATHER DISASTERS** IN THE US SINCE 2000 HAVE OCCURED IN JUST THE **LAST 3-4 YEARS.**[4]

INNOVATION

IoT Devices

Global Population

There are exponentially more connected devices than the global population. Our new, **interconnected risk** paradigm requires more agile, innovative and informed risk management and regulatory frameworks.

The EU's General Data Protection Regulation (**GDPR**) went into effect in May 2018 while California's Consumer Privacy Act (**CCPA**) will take effect in January 2020[5]. Going afoul of these rules will have costly ramifications for businesses.

Meanwhile, **blockchain technology** has matured in the last five years, offerring applications that can address data privacy concerns, supply chain risks, and disaster recovery efforts.

[1] https://public.wmo.int/en/media/press-release/greenhouse-gas-concentrations-atmosphere-reach-yet-another-high

[2] https://www.nationalgeographic.com/environment/2019/02/2018-fourth-warmest-year-ever-noaa-nasa-reports/#close

[3] https://oceanservice.noaa.gov/facts/sealevel.html

[4] https://www.c2es.org/content/extreme-weather-and-climate-change/

REPUTATION RISK

Trust is worth more than gold in today's business environment. To lose consumer trust is to face rapid and significant economic consequences.

Consider the **millions** lost by CBS, Netflix, and other organizations after high-profile #metoo accusations.[6]

These costs accumulate from legal fees, reduced market value from lasting reputational harm, and lost productivity from inside these organziations impacted by harassment and inequity.

POLITICAL UNCERTAINTY

Increasing political uncertainty – from the U.S.-China trade war, to Brexit and the return to economic nationalism globally – is impacting how enterprises do business. Fallout from the trade wars is expected to slow global growth to just 3% - the slowest in 10 years.[7]

CYBER RISK

Cyber breaches now impact billions of individuals each year. Financial data, health records, and consumer preferences have all been compromised to the tune of $1 trillion in 2018.[8]

A significant number of cyber attacks, over 40%, are on small businesses, and it can take nearly 6 months to detect a breach. Yet more than 77% of organizations have no cybersecurity strategy in place.

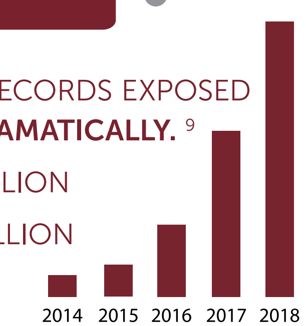
A HACKING ATTACK HAPPENS EVERY **39 SECONDS** IN THE U.S.[8]

ON A YEARLY BASIS, **EVERY THIRD PERSON** IN THE U.S. IS AFFECTED BY HACKER ATTACKS.[8]

THE NUMBER OF RECORDS EXPOSED IS **INCREASING DRAMATICALLY.** [9]

2004-2013 | 4.8 BILLION

2014-2019 | 11.6 BILLION



[5] https://techcrunch.com/2019/11/14/californias-new-data-privacy-law-brings-u-s-closer-to-gdpr/

[6] http://curmudgeongroup.co/quantifyingamovement/

[7] https://www.reuters.com/article/us-imf-worldbank-trade/fallout-from-trumps-trade-wars-felt-by-economies-around-the-world-idUSKBN1WY0PZ

[8] https://www.cybintsolutions.com/cyber-security-facts-stats/

[9] https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

Summaries

GUN OWNERS AND PERSONAL LIABILITY INSURANCE: A VITAL TOOL IN THE BATTLE AGAINST MASS SHOOTINGS | PUBLISHED 10.07.2019

Written by Les Williams and Andres Franzetti
Originally published on Risk & Insurance

The shooting in El Paso, TX added a new dimension to the gun control debate. Mexico may hold the U.S. responsible for the death of its citizens, opening up a new area of liability that U.S. companies involved in the high-risk business of selling firearms would be wise to insure against.

Read the full article: https://riskcooperative.com/news-and-analysis/americas-global-security-problem/

CYBERVISTA: EXECUTIVE BRIEFING ON CYBER INSURANCE | PUBLISHED 09.09.2019

Featuring Les Williams
Originally published by CyberVista

Dubai has instituted a unique digital transformation journey–the goals are not profit or efficiency, but happiness. Smart Dubai puts citizens at the forefront, supported by political leadership and a whole-government strategy to reduce the friction between citizens and government.

Watch the video: https://riskcooperative.com/engagements/cybervista-briefing-cyber-insurance/

RC QUICK TAKES—EQUIFAX BREACH | PUBLISHED 08.06.2019

Written by Andres Franzetti
Originally published on RiskCooperative.com

As the October 31st deadline for a Brexit deal draws near, the specter of post-Brexit consequences is becoming more and more real. Risk Cooperative CEO, Andres Franzetti offers his take on the risks to organizations from uncertainty and economic nationalism.

Read the full article: https://riskcooperative.com/news-and-analysis/rc-quick-takes-equifax-breach/

CATALOGUING AND CATALYZING BLOCKCHAIN FOR IMPACT | PUBLISHED 05.22.2019

Written by Dante Disparte
Originally published on Forbes.com

In a landscape where up to 92% of blockchain projects fail, where are the successes? Cataloguing and Catalyzing Blockchain for Impact is one way to get a sense of the social impact the technology is having around the world.

Read the full article: https://riskcooperative.com/news-and-analysis/cataloguing-and-catalyzing-blockchain-for-impact/

Links to all RC published articles, interviews, and engagements are located under Insights on riskcooperative.com.

Featured Analysis

3D RISK MANANGEMENT: A SURVIVORSHIP FRAMEWORK | PUBLISHED 05.16.2014

2014

Written by Dante Disparte
Originally published by the American Security Project

For most firms risk management is a necessary evil, increasingly consigned to being an adjunct to compliance, finance and other so called "business prevention" functions. Non-financial firms traditionally address risk through a series of transfer mechanisms, such as insurance, self-funded vehicles or they merely absorb unforeseen losses with their earnings. The financial sector, on the other hand, applies sophisticated statistical methods in a form of speculative risk management that captures the upside and the downside of risk-taking. These approaches are used to calculate value at risk (VaR), regulatory capital and other internal and external risk measures. Many of these methods, however, are based on backward looking book values and a permissive fox watching the chicken coop environment, wherein financial institutions often develop their own internal risk metrics with loose guidance from regulators.

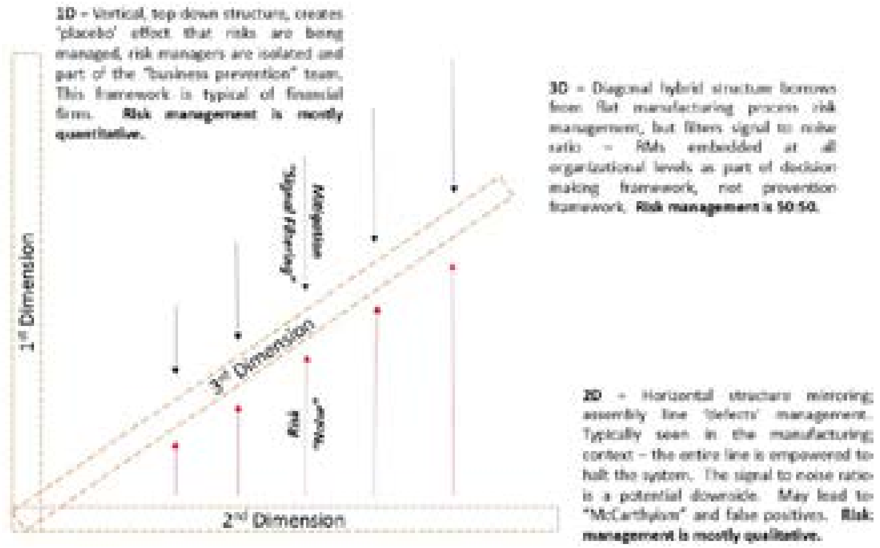
The frequency of potentially preventable losses, along with the calamitous effects of black swans, suggests that quants not only need qualitative tools in their arsenal, they need structural alternatives to one-dimensional risk management. This one-dimensional structure often misses the mark and can suffer from confirmation bias in that centralized risk managers who look for trouble, may in fact find it by chasing misleading risk signals. JP Morgan, long considered a best practitioner in banking risk management, missed the London Whale's transgressions, despite some fairly obvious warning signs1. Under the first dimension, even though many firms like JP Morgan install 'native' Chief Risk Officers (CROs) in their business lines, these individuals are often marginalized and kept on a need-to-know basis. This has the placebo effect of creating a false sense of comfort that risks are being managed, when in reality often excessive risk-taking behavior is carried out in the CRO's line of sight. The latency and backward orientation of traditional risk measures often negates proactive controls and when the smoke begins to rise, it is often too late.

One-dimensional risk management follows a hierarchical command and control structure. This not only creates isolation compounded by the vast remoteness of global firms, in most cases, CRO's report directly to the excessively optimistic CEO's they are supposed to manage. This was the case with JP Morgan, as Jamie Dimon, JP Morgan's all-powerful Chairman and CEO, pushed the boundaries of the firm's internal hedging activities carried out by its Chief Investment Office (CIO). For a one-dimensional approach to be effective, studies have found that the one variable firm's cannot compromise on is to have an independent board-level risk management regime2. In cases where CRO's report directly to the CEO and not the board, "paycheck persuasion" is a powerful inducement not to ring the alarms too loudly or to turn a blind eye to egregious behavior.

The robustness of risk management in the financial sector has a spotty record due to the wholesale collapse and public bailout of the system during the recent financial crisis. This is compounded by the implicit or explicit mandate given to risk managers to merely toe the regulatory line and do what is minimally required in terms of solvency, capital buffers and other standards. Indeed, many analysts suggest that JP Morgan's London Whale debacle was driven by persistent regulatory arbitrage to reduce the

Featured Analysis

risk-weighting of its capital buffers3. In short, meeting externally imposed compliance standards does not bode well for survivorship. In fact, under persistent conditions of economic duress, such as those seen during the recent crisis, which is defined as a 40% collapse of U.S. equities, even the mightiest institutions would fall. This not entirely improbable scenario would see another instance of privatizing gains, while socializing losses – this time to the tune of 598 b.USD for the top 10 systemic firms in the U.S. to fill their capital shortfall4. In short, doing what is minimally required by the regulator under a one-dimensional risk management structure is a risky business.



While risk in financial firms makes for headline news and has broad public interests as banks are increasingly viewed as utilities, preventable losses and missed signals as not confined to Wall Street. Toyota's ascendance as a global automotive powerhouse has hit a few speed bumps following a series of worldwide product recalls, sticking accelerators and an embarrassing mea culpa by Akio Toyoda, Toyota's CEO. Long heralded as the paradigm for kaizen, or total quality management, Toyota's assembly line follows a horizontal, or two-dimensional, risk management structure. The aim is to reduce the probabilistic incidence of errors in the manufacturing process to as many standard deviations as possible, for example 6 sigma. Famously, this two-dimensional structure empowers workers on the assembly line to pull the cord, in effect stopping production in the event of an error or pattern of errors.

Although many aspects of this flat structure are appealing, it labors under a potentially high "signal to noise" ratio that may lead to false positives and may only be applicable to firms or markets with a slower velocity. For example, it is doubtful that a two-dimensional risk management approach would have saved the high-velocity trading firm Knight Capital, which crashed and burned with spectacular speed due to a rogue trading algorithm. Besides, tracking defects is a slightly more gratifying task when you have a tangible product. In financial services, however, defects are occluded by correlations and their formless nature. Much like a virus, financial risk is often identified through contagion and rising temperatures, neither of which are sound preventive measures. Despite all the passive and active safety features in a modern car, externally imposed speed limits and driving conditions, there is no risk management substitute for a well-trained driver. Similarly, most risks in financial and non-financial firms emanate from the behavior of people inside the firm and in the market.

Against this backdrop, a hybrid third-dimension of risk management offers a new framework for an increasingly punishing and interconnected world. In this approach, risk management is not merely a quantitative preventive feature, but rather an embedded firm-wide decision making framework that makes staying in business, everybody's business. Leveraging the best of the first and second dimensions will filter signal to noise and encourage bounded risk taking at all organizational levels. The power in this approach lies in combating complexity with simplicity and removing the stigma of raising the alarm. Some of the more enduring risk management precepts take a via negativa or, subtractive path, prescribing actions that should be avoided, for example, thou shalt not kill. Imagine the power, clarity and resilience of the Volcker Rule, which in 1077 pages precludes proprietary trading, if it was simply stated as thou shalt not speculate with other people's money – the very egregious behavior that got JP Morgan into trouble.

[1] Robert Kaplan, et. al., *JP Morgan's Loss: Bigger than "Risk Management"*, HBR Blog Network, May, 23, 2012.

[2] Senator Carl Levin, Chairman, et. al., *JP Morgan Chase Whale Trade: A Case History of Derivatives Risks and Abuses*, Permanent Subcommittee on Investigations, U.S. Senate, March, 15, 2013 Hearing.

[3] Jon Macaskill, *Rivals Hover over JP Morgan as Farce Threatens to Turn into Tragedy*, Euromoney, June, 2012.

[4] Acharya, et. al., *Capital Shortfall: A New Approach to Ranking and Regulating Systemic Risks*, AES Meetings, January, 7, 2012. NYU Volatility lab systemic risk rankings http://vlab.stern.nyu.edu/welcome/risk/

https://riskcooperative.com/news-and-analysis/3d-risk-management-a-survivorship-framework/

IT IS TIME FOR A CYBER FDIC

| PUBLISHED 01.06.2015

2015

Written by Dante Disparte
Originally published by the American Security Project

In today's modern frictionless economy, the principal requisite for growth and order is the free flow of sensitive information, banking transactions and private data on a global scale.

With this shift brought on by the unrelenting growth of ecommerce and mobile platforms comes the nagging reality that cyber risk is here to stay. It is the sort of drag on the market that needs to be priced into the system rather than treated like something that can be eliminated or perfectly controlled. Market and consumer expectations need to be adjusted accordingly and in the age of hyper transparency, people would be wise to remember that anything can be exposed to sunlight.

Much like bank's zero-liability policies largely defanged identity theft and the risk that consumers would be saddled with thousands in losses due to phishing scams and fraud, so too cyber risk needs to be neutralized by a broad consensus on how to shift risk and respond appropriately. Perhaps it is time for a cyber Federal Deposit Insurance Cooperation (FDIC) to shore up confidence and risk-bearing in the system.

While the fallout from Sony's breach is still unfolding, especially as litigation is being drawn up by past and current employees, it is likely that Sony's besmirched reputation and consumer confidence will be the true victims of this attack.

RISK MATTERS | FALL 2019

Featured Analysis

Although Sony's cyber attackers have threatened even more havoc following the release of *The Interview,* experts estimate the economic cost of this attack to be between 1% and 2% of Sony's $22.5 billion market capitalization – hardly a death blow to this massive enterprise. Yet, Sony's attack raises the specter of state-sponsored cyber terrorism, against which no private firm can marshal a strong countervailing system. Coping with this risk requires new standards of practice to emerge around an early warning system, destigmatizing the advent of breaches and capping liabilities when they occur.

All of this can be achieved through cross-sector collaboration between the government and the private sector, much like the conditions that gave rise to the FDIC following the Great Depression. In short, cyber risk should not be treated like a discrete risk for individual firms to deal with on their own. Cyber risk needs to be treated like a threat to national security requiring a strong collective response and measures to shore up the system.

The FDIC is regarded as one of the most effective and enduring Federal agencies and its services, much like a centralized cyber risk pool, are not free. Banks pay risk premia based on their balance sheet, solvency and other factors. These funds are then used to shore up the broad system against bank failures and protect consumer accounts up to $250,000. Following the Great Depression and the wave of bank runs/failures, the FDIC provided a vital safety net and restored confidence in the system. In addition to the powers of restoring trust and capping exposures, a cyber FDIC must also carry strong deterrent powers in coordination with other U.S. government agencies. In short, speak softly and carry a big stick is an apt description and cyber ne'er-do-wells should face proportionate applications of U.S. power for their misdeeds.

When the Terrorism Risk Insurance Act (TRIA) was drawn up following 9/11, cyber risk was in its infancy and, as a result, was not contemplated in the Act, which was designed to shore up mature property and casualty insurance markets and transfer catastrophic losses to the Federal government.

The fact that Sony's business model was successfully held for ransom by Guardians of the Peace, as their attackers call themselves, shows that this risk category has come of age and our national response needs to keep pace. Ironically most firms go it alone when they learn of a breach – if they learn about this silent menace at all. This omerta is a byproduct for fear of a public and employee backlash over the exposure of private data and trade secrets – a silence that makes the overall system weaker, under the guise of risk and crisis management.

It is a simple, if painful truth, that holding on to bad news does not dissipate its impact, it makes it worse. Therefore, the final aspect of a cyber FDIC would be to run a central risk reporting clearing house that would collect system-wide information on breaches, near misses and comparative data across time. This last function would not only help mitigate cyber risk, it would also help improve private sector risk pricing and appetite as the industry still labors under limited historical data for this relatively new risk domain.

https://riskcooperative.com/news-and-analysis/it-is-time-for-a-cyber-fdic/

AMERICA THE RESILIENT

| PUBLISHED 12.14.2016

2016

Written by Dante Disparte and Stephen Cheney
Originally published on International Policy Digest

The United States and indeed the world are entering a period of great turbulence with unforeseen consequences at every turn and cascading events at every failure to anticipate risk and pre-invest in resilience. Resilience as a national priority is defined by the ability to withstand and spring back from shock events and attritional losses.

Our oceans no longer shield us from distant enemies and the days of Fortress America have been replaced by vulnerability to global shocks and insidious threats of the man-made, natural and emerging variety. A mere mosquito bite half a world away and a wayward traveler imports the next human pandemic. Our policymakers, political, military and business leaders can no longer debate or search for causality for these grave changes, we must now respond to their impacts and do so in a concerted, collaborative and urgent way. The role of the private sector in building a resilient society is as stark as it was during the industrial revolution.

30 years ago, when black swans (large scale risks) were still rare enough for us to ignore them, it made sense for our counties, cities and states to pick up the pieces, dust themselves off and rely on Federal disaster assistance to rebuild. Today, with sovereign debt presenting an emerging threat to national security, black swans are not only increasingly commonplace, they appear to be flocking around our country and coming home to roost.

Boston's record shattering snow fall, California's perennial dry spell, wildfires and noxious methane leaks that displaced thousands of Los Angelinos, are but a few recent examples of the convergence of man-made and natural risks. We have not only reached a tipping point, we are sliding off the other side.

Katrina, Irene, Sandy and, more recently Patricia, the most powerful hurricane ever recorded, have set their sights on iconic U.S. cities. The internally displaced people (IDPs) from the Gulf region and New Orleans in particular, remind us that large scale human resettlement is no longer the scourge of developing countries, but a part of our reality in the U.S. and something for which we are emotionally and materially unprepared.

Sadly, a platform based on long term resilience will not get a politician elected in our times of gridlock and internecine fighting. Yet, resilience is the key issue defining our future and something each citizen must demand of their elected officials. Each entrepreneur and business leader should set their ingenuity free with resilience as their market focus. The water crisis in Flint Michigan underscores just how fragile we are and supports the argument that resilience must become an investment-grade asset class. Resilience on the vast scale required in the U.S. can be measured as an investment opportunity in the sum total of our human, physical, response and technological systems. In order for this asset class to emerge, the traditional investment horizon needs to be stretched much further than 5 or 10 years and go well into 30, 50 and 100 year spans.

Resilience is an investment in which the investor may not be around to enjoy the returns, but there is no other asset class based on so much certainty. Our world is changing and we must invest trillions in being prepared – no sector has this purchasing

Featured Analysis

power and patience like large pension funds, hedge funds and insurers.

Unfunded losses that are passed on to the Federal and state balance sheet through agencies like FEMA, the CDC or the military are not sustainable in the long run. In a resilient society, these vital agencies would be the suppliers of last resort and not the first responders – after all, these are often the costliest interventions we have when combating a crisis. Some crises, like the Great Blackout of 2003, which sent 55 million people in the Northeast and Canada into darkness are so insidious they are triggered by tree branches touching high tension power lines in Ohio. Sending the Army Corps of Engineers to prune trees along the U.S. electrical grid is a costly proposition that comes at the price of our global security posture, even though they would get the job done.

Instead of waiting on the sidelines and responding to and funding shocks as they emerge, we must begin to anticipate and prefund them along the entire spectrum of risks one county and city at a time until we have a tightly woven resilient fabric protecting our society. From this platform of endurance, we can continue to lead global efforts having pioneered the new industries and methods for human adaptation.

The central question of building a resilient society is not one we are accustomed to asking – namely, who pays for it? In seeking answers, we came across the Lloyd's City Risk Index a scholarly work in conjunction with Cambridge University. It provides a measured framework for quantifying the economic value at risk in 301 cities around the world comprising more than 50% of global GDP, including 29 cities in the U.S. In all, there is $7.33 trillion of economic output at risk in North American cities to 18 man-made, natural and emerging threats. Behind these figures, countless lives and livelihoods are at stake. Resilience is the challenge of our time and an asset class worth investing in – doing so requires mobilizing all stakeholders to get off the sidelines and begin demanding long term change and investment.

https://riskcooperative.com/news-and-analysis/america-the-resilient/

SIMPLE ETHICS RULES FOR BETTER RISK MANAGEMENT | PUBLISHED 11.08.2016

2016

Written by Dante Disparte
Originally published on Harvard Business Review

For far too long, managing risk has been seen as an esoteric business function — designed to control losses and adhere to compliance standards. But as more organizations fall prey to complex intangible risks, from unwanted disclosure due to rampant cyber threats to breaches of conduct driven by skewed incentive systems, the aperture of risk management is expanding from protecting the balance sheet to promoting ethical leadership and values-based decision making.

Consider Yahoo, with its record-breaking cyber breach estimated at more than 500 million records, or Wells Fargo, facing unwanted public excoriation after creating thousands of fake customer accounts, or the Volkswagen emissions scandal or the warning signs that could have prevented the Germanwings disaster. Many of these failures were either fueled by or lost in the byzantine maze that is the modern enterprise, which often breeds a combustible mix of indifference and short-termism. Complex systems fail in complex ways. But all start with human failings.

Senior business leaders and their boards must therefore change the way they think about risk and how they respond to it. Rather than countering complex risk with an even more complex risk-management system, which comes with its own blind spots and brittle places, leaders have to equip the individuals in their charge with common levels of risk awareness, codes of conduct, and value systems.

To do this, I've often relied on a handful of maxims. While it's true that maxims can sometimes sound cliché – like a phrase on a motivational poster that employees walk past every day but never really look at — they can also be useful if leaders put real muscle into them. Here are a handful that I have found most useful in fostering a healthy sense of risk-awareness in organizations in which senior managers are themselves also demonstrating ethical leadership:

Values matter most when they are least convenient. In an environment riddled with uncertainty and variability, value systems are meant to be the only constants. However, all too often they are proven to be meaningless words in an annual report. For value statements to be more than empty slogans, they must withstand the trial by fire of tough calls guiding behavior and decision making when it is least convenient. The now famous Tylenol recall of the 1980s is an enduring example of how Johnson & Johnson's credo guided decision making in a time of crisis. A small number of firms are counter-intuitively becoming activists about championing their value systems, even at the risk of short term shareholder returns. No one gets extra credit for doing the right thing when it is easy.

Bad things happen in the dark. Ethical lapses arise when people take risks but do not bear the downside of their risky behavior. These hazards are most prevalent where they can be most easily hidden – such as in remote locations, less-supervised business units, or on understaffed teams. Misaligned incentives can also create organizational "blind spots." Wells Fargo's massive account-rounding scandal illustrates the insidious effects of incomplete employee incentives that turn a blind eye to unethical behavior.

Combating issues like these begins with transparency and accountability. When information is shared quickly and openly across the organization, bad

RISK MATTERS | FALL 2019

Featured Analysis

dealings can be rooted out before they spread. It's leaders' responsibility to shine a light into any dark organizational corners.

Privacy is a luxury. In the age of pervasive cyber-risk and unwanted disclosure, consistently aligned behavior is the best defense. All it takes is one employee clicking on one sketchy link in one email for an organization or institution to be infiltrated by anyone from a disgruntled employee, to WikiLeaks, to nation state actors. The recent large-scale denial of service attack that affected internet stalwarts like Amazon, Twitter, and PayPal by exploiting connected devices underscores that the amount of money spent on cyber security is not a proxy for greater defense. The Clinton campaign spent months of time and effort atoning for statements made in emails sent through Hillary Clinton's private server, and continues to respond to emails hacked by, allegedly, the Russian government and leaked through Wikileaks. Apparently, the hackers were able to get access to the emails when campaign chairman John Podesta clicked on a phishing link.

Today, risk lies between the chair and the keyboard. Given that breaches are now seemingly inevitable, risk managers might need to spend less effort trying to prevent the next hack and more time reminding employees not to include embarrassing or sensitive information in easily-breached communications in the first place.

Remoteness breeds indifference. Attitudes toward risk are deeply informed by the tone, tenor, and remoteness of the top. Leaders who practice what they preach, have conviction, and lead by example are better at managing risks than those that merely pay lip service to ethics, value systems, or codes of conduct. Simplicity is key in addressing this gap. When senior leaders encourage bounded risk-taking and show that they are open to hearing bad news, they can help hone an organization's muscle memory –on how to respond to emerging threats. When those executives conversely dismiss details as too "in the weeds" for their attention, show that they don't want to hear questions or bad news, or are simply impossible to ever track down in the hallways, moral lapses become more likely.

Remember the example of Citibank from the 2008 housing crash – Kellogg professor Adam Waytz found that leaders in New York were both physically and psychologically distant from whistleblowers in Missouri and Texas. No significant actions were taken to curb the improper behavior, and the company had to pay a $158.3 million settlement in 2012.

Just as David was able to slay Goliath with a simple sling, complex risks are best addressed with simple measures. Firms should not embrace ethical leadership or risk agility out of fear of failure or mere compliance. Risk agility is a source of lasting competitive advantage. After all, when the competitive landscape is littered with the tombstones of firms that failed to understand and respond assertively to risk, the ethical and agile enterprises will inherit the spoils.

https://riskcooperative.com/news-and-analysis/simple-ethics-rules-better-risk-management/

BLOCKCHAIN AND THE POWER OF SINGULARITY | PUBLISHED 01.08.2017

2017

Written by Dante Disparte
Originally published on Huffington Post

Set on Sir Richard Branson's Necker Island, the third annual Blockchain Summit, hosted by BitFury, a leading full service Blockchain company, and Bill Tai, a venture investor and technologist, has come to a close. This event was an intimate, if perfectly balanced, gathering of technology, policy, investment and business leaders from around the world and across sectors. Topics ranged from the public policy implications of what is being heralded as a foundational technology, to new emerging business models that can ride on the very rails that enabled the global bonanza of digital currencies like Bitcoin. A key question that underpinned the Summit is if Blockchain could not have existed without the Internet, what could not exist without Blockchain?

Blockchain technology can undoubtedly change industries, especially those that labor under often byzantine, opaque and friction-laden business models. While many of the early pioneers are focusing on finance and insurance, the opportunities for this radical technology may very well reorder society as we know it. The remarkable case of Estonia, for example, shows a country reinventing itself into a future-proof digital state, where citizen services are rendered nearly instantaneously and to people all over the world. Similarly, promising work inspired by the famed Peruvian economist, Hernando de Soto, on improving land registries is being carried out by BitFury in a host of countries. With land and property being the two largest assets people will own - and the principal vehicle of value creation and wealth transfer - an unalterable, secure and transparent registration process should give the world comfort and elected leaders longevity.

What drives this unique technology is the power of distributed singularity, from which Blockchain's identity pioneers like Dr. Mariana Dahan, who launched the World Identity Network on Necker Island, and Vinny Lingham of Civic, draw their inspiration. Blockchain operates on the basis of a distributed ledger (or database) system, inexorably marching forward recording and time-stamping transactions or records. While some may herald Bitcoin as Blockchain's "killer app," it is easy to maintain that the killer app is not the digital currencies that ride on Blockchain's rails, but rather the rail system altogether. Two trains can ride on rails. But a high-speed maglev train is a decidedly faster mode of transport than a steam engine. Just as the maglev makes little or no contact with the rails enabling low-friction transport, the Blockchain can greatly reduce the friction in how the world transfers and records value. If the Internet augured frictionless information sharing, Blockchain can augur frictionless value transfer. Herein lies the domain of truly profound change - accepting that Blockchain is still in the era of a thousand flowers being planted, many of which began blossoming on Necker Island.

For now, the Blockchain standards war - which in reality is an incredibly collaborative search for use cases - is largely being waged in the cash transfer market, with firms like Bitt, founded by the Barbadian entrepreneur, Gabriel Abed, and BitPesa, founded by Elizabeth Rossiello, emerging with low-friction highly scalable business models. What is most encouraging is that these firms, have not shied away from regulatory regimes, but rather embraced them, greatly legitimizing the

RISK MATTERS | FALL 2019

Featured Analysis

poorly named crypto currency market. BitPesa has received UK regulatory approval from the Financial Conduct Authority (FCA), which is one of the most stringent financial regulators in the world, while Bitt has created a veritable pan-Caribbean digital currency accepted by many regional central banks. In short, digital currency and frictionless asset transfer are not going away and the more pioneers like Bitt and BitPesa harmonize with established financial norms, the more this space can thrive.

The Blockchain Summit on Necker Island was all about encouraging breakthrough innovation across all sectors. If the Internet was truly a disruptive technology, Blockchain is an augmenting technology, that can greatly improve and amplify many established business models and forms of governance. At a time when the world is gripped by profound changes driven by an erosion of public trust in business, institutions and government, a trust engine like Blockchain can begin to shore up accountability and transparency. Similarly, with rampant cyber-threats hobbling companies and countries around the world, Blockchain cannot only serve as a vital source of transparency - recalling that sunlight is the greatest disinfectant - it may very well serve as a global disaster recovery and business continuity engine. Blockchain's security properties are often undersold, however, these are among the most important features of this technology. Indeed, hardwired into Blockchain's distributed structure are the very best practices of cybersecurity redundancy that so many organizations struggle to abide by.

Where minds begin to race when it comes to Blockchain and where Blockchain Billionaires will likely emerge, is in the unitary approach (and smart contracting features) to value transfer. The sharing economy has undoubtedly tapped people's willingness to forego traditional asset ownership for fractional, usage-based access. Blockchain takes this intuition even further by enabling these same market dynamics to occur, but on a rail system robust enough to survive in Thomas Friedman's hot, flat and crowded world. Envision a skills engine enabling people to repurpose themselves, obtaining vital (verifiable) credentials to enter the workforce or to find work following a setback or job loss? Without Blockchain this proposition is not only cost prohibitive, it is incredibly centralized favoring a dated algorithmic hiring model that has left millions of workers behind. With Blockchain, this type of "reinvention engine" is not only possible, it can be developed with sufficient autonomy and transparency across stakeholder groups ultimately becoming a utility.

Indeed, one of the most promising companies focusing on Blockchain applications is PowerLedger in Australia, which was founded by Dr. Jemma Green. Dr. Green, traveled more than 40 hours carrying her young daughter in hand and her weight as one of the world's true Blockchain visionaries. Her firm taps the power of singularity and decentralization in the Blockchain, as well as underscores the ability to harness renewable energy in ways (and in places) never thought possible. Fractionalizing urban energy is as important to human adaptation and development, as building a rural energy matrix that incorporates micro grids and new distribution and payment models. PowerLedger is well on the way toward solving this challenge and Blockchain will be at the center of both.

Blockchain is here to stay and the exuberance of its most ardent enthusiasts (who are on the verge of a Bitcoin "civil war"), of which there were many on Necker Island, should be tempered with the reality that all breakthrough innovations are decided by the market. For this, large firms and established models of organizing and transferring value have been cautious to dismissive of Blockchain. This posture may consign many of these players to the wrong side of history, or worse, irrelevance. Indeed, the emergence of global industry bodies like the Global Blockchain Business Council, which is quickly establishing chapters around the world, as well as the Blockchain Trust Accelerator, are aiming to normalize this technology and, critically create a lexicon and library of use cases that are not threatening in the world's halls of power.

https://riskcooperative.com/news-and-analysis/blockchain-power-singularity/

FACEBOOK BREAKS SILENCE
| PUBLISHED 03.22.2018

2018

Written by Dante Disparte
Originally published on Forbes.com

The coat of Teflon that usually shields Facebook and its affable leader, Mark Zuckerberg, who has matured into a techno statesman in the public eye, is beginning to wear thin. Facebook now joins a growing number of firms embroiled in a trust deficit with a case of reputation risk whiplash. But unlike an Equifax-style scandal, which was prompted by external factors and exacerbated by internal misdeeds, Facebook's eroding market confidence appears to be self-induced by 5 days of silence and lax third-party risk management. Reports of more than 50 million personal records being accessed by Cambridge Analytica and Aleksandr Kogan, a Cambridge University researcher whose personality quiz provided a backdoor to this data, is not only a terrible violation of consumer privacy, it highlights how trust (the new thrift of the modern economy), is hard to earn and easy to lose.

Although Facebook has been no stranger to global privacy and security concerns, it has largely survived past scandals unscathed continuing its unrelenting march to social media dominance with more than 2.2 billion monthly active users. This time, however, the nature of this massive privacy violation has people like Brian Acton, who Mr. Zuckerberg made a billionaire with the $19 billion acquisition of WhatsApp, committing the treacherous act of joining the delete Facebook campaign on that other controversial social media platform, Twitter and elsewhere. The scandal, which Facebook has been silent about until Mark Zuckerberg released a statement on the platform, has eroded shareholder value by 8% or $35 billion. While the stock will surely

RISK MATTERS | FALL 2019

Featured Analysis

recover given Facebook's sheer dominance of the social media world, earning back consumer and regulatory trust will be hard fought.

Want it or not, Facebook has now become a protagonist on both sides of the Atlantic in the battle to restore trust in democratic institutions and privacy standards. Firms like Cambridge Analytica, with the grotesque videotaped admission from its crestfallen CEO Alexander Nix, made money in exploiting people's private information fueling election malfeasance in the U.S. and elsewhere. While Mr. Zuckerberg's apology tour is just beginning following his statement and planned interview on CNN, it will not be long before Facebook must heed calls for hearings with lawmakers and regulators in the U.S. and UK. These inquiries will dive deeper into third-party vulnerabilities on the platform, potential legal liabilities and other restrictions, which may challenge the firm's revenue model further eroding trust. The advent of GDPR, the EU's far-reaching privacy regulations, which take effect in May of 2018, along with the likelihood of an EU digital tax levied on firms like Facebook will only serve to compound Facebook's trust and compliance challenges. Critically, GDPR grants EU citizens the right to be forgotten.

While 50 million records is a rounding error for a firm of Facebook's network size, the nature and apparent ease with which these data backdoors were opened by third-parties will create lasting discomfort and scrutiny. The notoriously media shy Mark Zuckerberg is facing a tough challenge of restoring trust in the unwieldy and vast expanse of the social network he built but is now larger than him. For all the unwanted scrutiny of Facebook and its lax privacy and security standards, individual users must also look themselves in the mirror and question their digital naïveté about Facebook's commercial motives. Facebook, like so many private enterprises that are busy providing services they aim to monetize under the guise of "social utility," are best used by people who are open-eyed about the tradeoffs. In short, the 2.2 billion users who voluntarily made Facebook a global census bureau should not be surprised by efforts to sway them and make money based on their online behavior.

Where a redline was crossed, however, was when Facebook was subverted as an instrument of foreign electoral intervention and social sabotage at scale. While Cambridge Analytica is clearly one of the culprits of this social engineering, many other firms and nation-state actors, like the Russian-backed Internet Research Agency, partake in the type of micro-targeting that Facebook and its billions of users have enabled. The world's social network may have to replace its user and privacy statements with a new social compact that restricts advertising and micro-targeting from a wide range of third-party users on a wide range of themes. Indeed, Facebook, like other technology firms, have demonstrated that they can abide by self-regulation and at speed when they banned advertisements for initial coin offerings (ICOs), which have been prone to potential investor fraud risks. If only the same prudence was demonstrated during electoral cycles and in protecting consumer privacy. Until then, social network users, like voters, should weigh their conscience, use their judgement and proceed with caution.

https://riskcooperative.com/news-and-analysis/facebook-breaks-silence/

AN AMAZON SURVIVAL GUIDE IS NEEDED
| PUBLISHED 11.19.2018

2018

Written by Dante Disparte
Originally published on Forbes.com

After much national fanfare, Amazon, the second firm to join the trillion-dollar club, has announced the new homes of its much sought after HQ2. Not one home, but two, as the search for a single single city has in fact split with Long Island City, New York and Crystal City, Virginia (now recast as National Landing), in the greater Washington, D.C. area, claiming victory. While there are certainly a number of disappointed city leaders throughout the country, from places as far flung as Puerto Rico to Miami, how Amazon's two new homes prepare for the arrival of a trillion-dollar behemoth in some respects requires an Amazon Survival Guide. This will help ensure that smiles are not only on Amazon's ubiquitous packages and at fawning ground-breaking ceremonies, but on the faces of job seekers, business and community leaders who must contend with a new market-making and market disrupting neighbor over the long term.

The D.C. region playing host to half of HQ2 is no surprise, in no small measure because Amazon's CEO (the world's richest man), Jeff Bezos, has already planted a substantial personal flag in the region, buying D.C.'s largest (and most expensive) private residence. Like all self-respecting billionaires, the allure of political power and perhaps even presidential aspirations, is a good reason to lay a foundation in the nation's capital. In Amazon's case, Bezos is slated to become one of the region's largest employers after the Federal government and adds to the Washington Post, which is the other regional asset he owns. The business logic is clearer still, especially as Amazon vies to expand its lucrative government and defense contracting business, along with the attendant logistical and market proximity benefits of establishing two hubs on the east coast. It is already being reported that the regional move opens a pathway for Amazon to win a $10 billion defense contract. In one fell swoop this would net out the direct investment cost of $5 billion, which was the promised investment in HQ2, not counting the subsidies both host cities provided in the vicinity of $2 billion. Like when Amazon bought Whole Foods for $13 billion only to have this sum netted out by share price increases, it is very likely Amazon's gains in subsidies, government contracts and increased valuation will quickly net out the direct investments in HQ2.

No stranger to home market unrest and negative externalities, Amazon and firms of its size and clout have grown accustomed to being lightning rod neighbors, including in the communities where they were founded. Recognizing this and the lingering impact large tech firms have had on distorting affordable housing markets, Jeff Bezos, through his philanthropic efforts, has allocated $2 billion to improving affordable housing and early schooling options. Addressing adverse market responses in this manner aims to turn frowns upside down reverting back to the smile on Amazon's packages. Similar largess may be needed in its new host cities, which are both plagued by affordable housing and other social issues.

The other considerable advantage that will accrue to Amazon from its bifurcated east coast HQ2 is the ability to more directly influence and inform national policymaking, particularly as it relates to emerging business models where Amazon is staking its claim. For example, the prospect of nation-wide drone deliveries means the drones must take off with FAA approval. A platform in the capital region

RISK MATTERS | FALL 2019

Featured Analysis

playing home to Jeff Bezos will be more amenable to allowing delivery drones to fly in lower, currently unregulated airspace. Seeing as helipads were thrown into the mix to sweeten site selection inducements, Amazon clearly intends to fly more than helicopters from these new locations – with National Landing in line of sight of D.C.s Reagan National Airport.

Similar market entry is taking place in healthcare especially as the triumvirate between Amazon, JP Morgan and Berkshire Hathaway evolves into a yet to be named company with considerable leadership in Dr. Atul Gawande at the helm. This health insurance platform that pools a combined 1 million employees from the three firms into a new insurance structure represents a major broadside to all industry participants. Nationalizing this framework into more direct competition with private health insurance and state or government-backed healthcare programs is more likely to receive a regulatory blessing with an influential east coast Amazon, notwithstanding the ructions between Jeff Bezos and President Trump, which took a turn for the comical on Saturday Night Live.

Beyond Amazon and the triumvirate leading a mass private health insurance opt out, the prospect of direct competition to health insurers from a tech titan, a banking titan and an insurance titan, could very well be the death knell to underperforming insurers. The jury will remain out on whether this is good for markets and consumers. What is true of the companies and employers operating in Amazon's shadow is that they now face a major double jeopardy, where they only have a few years to begin preparing. On the one front, no public or business leader wants to unfurl the "unwelcome mat" to an investor that stands to hire a combined 50,000 employees in host cities – or at least this much was asserted in pre-investment promises. To this welcoming committee, getting into Amazon's value chain and gaining the economic competitiveness that Amazon represents can be a boon. On the other hand, Amazon's 50,000 new hires, especially in the highly competitive and already costly D.C. market, will come at the substantial expense of regional employers, who are already involved in a fierce hiring and retention knife fight for top technical talent. Indeed, one of the insidious aspects of the D.C. area job market, is that many facets of the Federal government and national security apparatus are in fact already privatized.

As with all economic growth, market displacement is the attendant consequence. For this, the first chapter of an Amazon Survival Guide, would outline business scenario planning for what the possible positive and negative impacts are likely to be. Like with all risk management, you cannot buy insurance when your house is on fire, no more than you can respond to Amazon poaching your top talent or your lucrative government contract the moment it happens. Risk favors the prepared. Similarly, firms that try to get into a spending war with Amazon on employee compensation and benefits risk engaging in a fool's errand. Instead, the value proposition of employment in these firms and government agencies must hinge on qualitative matters where more money is not a proxy for higher employee engagement, satisfaction and, critically, loyalty.

The other known and expected negative externality of a friendly neighborhood Amazon is depletion of affordable housing stock and rapid appreciation of existing inventory. In both homes for HQ2, the lack of affordable housing is already an endemic issue. In national terms, the greater Washington area is rivaled only by Hawaii in terms of rental costs. Would-be urban dwellers – those who want to avoid the region's nightmarish traffic – need to earn at least $33.58 an hour in order to afford the rent for a 2-bedroom apartment. In New York, the same figure is $28.08, not to speak of challenges in home ownership in both markets, let alone nationally. While these issues are not directly Amazon's fault, and no one should begrudge Amazon's success, policymakers, particularly those who care about affordable housing and containing the unintended side effects of unbridled gentrification, balanced measures will matter.

If the first chapter of an Amazon Survival Guide is about what market and regional leaders can do to prepare, the second chapter would shift the onus to Amazon and outline ways the firm and its patron can become locally engaged citizens. In both of its new homes, Amazon moves into highly stratified regions along economic, social, educational and ideological lines. Deploying Amazon's considerable social and financial capital into ameliorating these issues including in the second city in the D.C. mega-region, Baltimore, can not only bend the arc of many of these young lives, it can bend the arc of the region toward long term economic competitiveness. This much was Amazon's chief motivation for moving eastward. While improving regional economic competitiveness is not singularly Amazon's burden to carry, what will soon become the region's largest employer after the Federal government, Amazon has a unique opportunity and, some may argue, an obligation, to make all ships rise in its wake.

https://riskcooperative.com/news-and-analysis/an-amazon-survival-guide-is-needed-2/

IT'S LONG PAST THE TIME FOR BANKS AND INSURERS TO UNFRIEND COAL. HERE'S WHY.

2019

| PUBLISHED 10.14.2019

Written by Les Williams
Originally published on Risk & Insurance

September 20 through 27 commemorated a historic week around the globe. According to the website GlobalClimateStrike.net, over 150 countries experienced protests supporting climate change initiatives. These protests were effective in keeping climate change at the forefront of our social conscience; now getting businesses on board will further amplify the message of a cleaner planet.

The Heat Is On

The Intergovernmental Panel on Climate Change (IPCC) is a working group of the United Nations tasked with assessing the science related to climate change. During its latest meeting in September 2019 in Monaco, 100 scientists from 30 countries met to discuss the latest science and effects of climate change on various ecosystems around the world.

According to the IPCC report, global warming has already reached 1 degree Celsius above pre-industrial levels due to the increase in greenhouse gas emissions. This has caused melting glaciers, rising sea levels, warmer and more acidic oceans, and more severe weather patterns.

Hoesung Lee, chair of the IPCC, stressed that although many of the regions studied in the report seem distant from humans (oceans, the Arctic, the Antarctic, high mountain regions), these regions impact the globe in ways such as climate, food, water, tourism, health and well being, travel, and more.

Featured Analysis

As an example of this interconnectedness, the thawing of Arctic permafrost, or frozen tundra, not only impacts the traveling and hunting patterns of indigenous peoples, it releases extreme amounts of carbon, contributing to the increased concentration of greenhouse gases on the planet. Climate change has produced dangerous environmental conditions impacting humans regardless of location on the planet — nothing, no one and no enterprise will be spared from the effects, hence the need for concerted action.

Being Greener, With the Influence of Green

Tying money to behavior is arguably the best way to produce favorable outcomes in many scenarios, including the creation of a cleaner environment. A recent article in Businessweek discussed how climate activists are focusing their attention on banks, which provide loans to major emission-producing companies. ING Group NV is one such bank that is working to determine which assets on its balance sheet are major contributors to global warming.

Financial institutions, such as ING, realize that climate change may be a hidden risk on their balance sheet; serious emitters of greenhouse gases may see a drop in their valuation due to changes in policy (i.e., a country issuing a mandate to suddenly and drastically decrease greenhouse gas emissions, and certain companies/industries are unable to pivot their operations quickly enough to meet the timeline). By targeting certain clients at-risk, ING is able to encourage these entities to literally "clean up" their act if they wish to remain clients in good standing.

Banks are not alone in this emerging role of creating a cleaner environment through decarbonization mandates. Businessweek unveiled a growing trend in the European business community, "Flight Shaming." Globally, airlines release approximately 1 billion tons of carbon dioxide. Due to pressure from climate activists in Europe, businesses across the continent are revamping their travel policies. More business travelers are relying on buses and trains to arrive at their destinations as their companies reduce the amount of flight reimbursement funds made available, and more meetings are occurring virtually via video or teleconference.

Airports in countries like Sweden have seen a drop in the number of passengers they serve, and this trend will continue in other countries as Europe's business community continues to respond to the changing cultural dynamics. Businesses may soon realize that by not adopting some changes to their airline travel policies, they may face a reputational risk, which could result in the loss of valuable clients. Add the likelihood that air travel will get a little bumpier and a little costlier in a more turbulent world, an "opting out" of all but essential business travel may be as good for comfort as it is for the bottom line.

Insurance as a Catalyst for Climate Change Reform
This past summer, the Bank of England's Prudential Regulation Authority (PRA) stated that it will work with UK insurers to determine how climate change will impact their finances. The PRA is the bank's regulatory body that supervises financial service firms like insurers. In a report released this past May, David Rule, the executive director of insurance supervision at the PRA, explained the plan is to help insurers "better assess, manage and report exposure to climate risks related to extreme weather events which in turn will lead to action."

California's insurance regulator has followed a similar posture, asking insurers operating in the state to conduct veritable climate stress tests on their balance sheets to not only identify climate change exposed assets but also recalibrate their liabilities. This is a part of California's broad climate-ready strategy, which calls for a 50% decarbonization of the state's energy production by 2030.

Given the impact climate change is having on insurance claims globally, the PRA is wise to investigate how climate change will impact the balance sheets of these insurers that directly has an impact on the bank's financial health. Historically, catastrophe models relied mainly on historical data for underwriting — models that are now outdated given the impacts of climate change.

The main goal of the report is to help insurers develop a more accurate, forward-looking underwriting model that accounts for the impact of climate change. By more accurately underwriting risks incorporating climate change, the PRA is encouraging insurers to take steps to remain solvent for decades to come. If we view business as an engine, capital would be the fuel and insurance would be the oxygen. As insurers step up to the plate and include climate change impacts into their underwriting models, more businesses will be compelled to make eco-friendly changes to their operations to secure favorable premiums or to secure any type of coverage in the first place.

Our industry has a key role to play in ensuring and insuring our planet remains cleaner for generations to come.

https://riskcooperative.com/news-and-analysis/climate-change-and-big-business/

A TWO-TIER HEALTH CARE SYSTEM COULD BE JUST WHAT THE DOCTOR ORDERED

2019

| PUBLISHED 08.19.2019

Written by Les Williams and Nara Rodrigues
Originally published on Risk & Insurance

Health care has dominated each of the 2019 Democratic Primary Debates. The first question posed to the candidates on July 30th in Cleveland focused specifically on a "Medicare for All" plan. The New England Journal of Medicine states that more than two-thirds of Americans feel that reducing health care costs must be a top priority for the federal government.

Politicians from both sides of the aisle agree with the sentiments of these Americans, but how to approach this intractable issue is the crux of the matter. There may be a compromise such that a Medicare for All Plan can coexist with the existing U.S. health care system.

Background of Medicare

Medicare was created in 1965 to help Americans aged 65 and older and those permanently disabled pay for medical coverage. Coverage includes services like prescription drugs, hospital stays, and doctor visits. According to the Center for Medicare and Medicaid Services (CMS), in 2016 Medicare covered over 56 million Americans at a cost of around $678.7 billion.

Medicare is funded via payroll taxes from employees and employers, self-employed individuals, income taxes paid on social security benefits, and interest earned on two trust fund accounts held by the U.S. Treasury. Medicare for All involves the idea of a single-payer system; in this case, the U.S. Federal Government footing the health care bill for all

RISK MATTERS | FALL 2019

Featured Analysis

Americans regardless of age. This would eliminate the need for private insurance (like Canada's system).

This stands in contrast to The Affordable Care Act (ACA), which simply helped more Americans access the health insurance marketplace that is still serviced by private insurers. While there are several derivatives of what a Medicare for All Plan would look like, the common theme among the Democratic candidates' plans involves the federal government's regulation of health care prices.

Proponents of a Medicare for All universe opine that government would be allowed to better-manage prices for medical care and prescription drug prices, while opponents argue that Americans should have the option to choose which health care plans they want for their families or, in the case of companies, their employees. These naysayers also feel that by having the federal government directly set health care prices, innovation in health care would be stifled.

What Businesses Think

Richard Master is the CEO of MCS Industries, the largest producer of picture frames, poster frames and framed mirrors in the U.S. You can find their products at major retailers including Lowe's, Target, Walmart, Amazon, The Home Depot, and more. While approximately 75% of MCS' 775 employees now work overseas, increasing health care costs have motivated Masters to support a Medicare for All National Plan. He is chairman of The Business Initiative for Health Policy (BIHP), an independent, non-partisan, public education and advocacy group focused on adopting Medicare for All in the U.S.

By allowing the government to manage health care prices, Masters argues that companies can focus on their core businesses and avoid the financial burden of providing health care to workers. Masters does not view Medicare for All through the lens of "health care is a right, not a privilege", rather he feels this single-payer system makes economic sense for businesses which in turn would help employees.

The Business Alliance for a Healthy California supports Masters' stance, the alliance stated that approximately 300 small businesses in California now back a single-payer system and the number continues to grow. Dan Geiger, the co-director of The Alliance, stated that larger businesses (i.e. Fortune 500 firms) have shown trepidation in joining the single-payer movement mainly because they want multiple options involved with choosing among various health plans for their workforce. They view it as an employee attraction/retention tool. The U.S. Chamber of Commerce agrees with the sentiments of these larger corporations.

In a letter to congress dated March 18, 2019, The Chamber argues that the federal government should take actions such as expanding the use of Health Savings Accounts to lower out-of-pocket costs, repealing the health insurance and medical device tax, expanding coverage options via mechanisms like Association Health Plans, and improving the existing ACA exchanges via funding cost-reduction initiatives. If things are at a stalemate in the U.S., can we learn from other countries?

Health Care from an International Perspective

Japan's non-profit health care system, called the National Health Insurance Model, is a highly successful program where the government is the single-payer of a single insurance plan while providers remain private.

In many countries, such as Japan, hospitals and physician groups are generally required to work on a non-profit basis. If a similar program were implemented in the U.S., there would be the risk of a decrease in health care personnel since U.S. providers have higher profit expectations than other countries. In Japan all citizens are required to enroll, and they receive free screening for several diseases (including prenatal care), and the only contributions made to health care costs are those that fall outside of a certain scope of service (at which point the citizen contribution is capped at 30%).

The government has tremendous bargaining power in keeping health care costs low in this model, and the program is highly successful with Japan having the second longest life expectancy in the world. Health care costs are kept at a low 8.5% rate of the country's GDP (lower than New Zealand, Germany, the UK, and several other OECD countries).

Despite the general success found in Japan, several countries that have some variation of a Medicare for All model usually deal with escalated inefficiencies, corruption, and low quality of care. It is also true that most countries with single-payer models experience higher waiting periods to see a doctor, as evidenced at The U.S. Department of Veterans Affair – an example of universal health care in our country.

The Best of Both Worlds

Implementation of another health care model will face challenges at many levels in the U.S.; politicians, pharmaceutical companies, doctors, hospitals, and citizens will offer strong opinions. Why can't we offer Medicare for All along with the existing privatized option to U.S. Employers?

Many companies in the U.S. segment their branding, Marriott owns The Ritz Carlton and The Courtyard Inn and prices them accordingly. From an employer point of view why can't the traditional U.S. Health care Model be viewed as a Ritz property, while Medicare for All is viewed as a Courtyard?

The opponents of Medicare for All feel that innovation will be stifled in this model given the government's control of health care costs.

Maybe a solution is having Medicare for All participating employers pay a tax called the "Innovation Incentive" added on their current payroll taxes. This fee could be deposited in a pool from which the research & development divisions at health care firms can draw from to pay doctors and scientists for the development of groundbreaking treatments. Marketing this as the "Innovation Incentive" leaves a better impression than simply a "tax" that Medicare for All opponents detest.

It is imperative to price this at an affordable cost for small companies, like MCS Industries. Options can bring out the best in business, so imagine a world where both health care models adopt best practices from one another creating a stronger overall health care system. It will take decades to see how a two-tier system unfolds in The U.S. once it is implemented, but it is an action worth taking for the health of our citizens.

It could be just what the doctor ordered.

https://riskcooperative.com/news-and-analysis/two-tier-healthcare-system/

RC Answers

Reviewing changes in risk managment provides valuable perspective. But what emerging trends should I embrace to prepare for the future?

As we celebrate five years in business, we have done our share of looking in the rear-view mirror at how the risk landscape has changed. Risks that were just emerging in 2014 are now commonplace. Add to this evolution the faster pace of change, and it's clear that we need to prepare now for what the future holds.

Every new year brings scads of opinions and articles touting the Top 10 risks for the coming year, but there are a few trends that are really worth embracing as part of your risk strategy.

Environmental risks related to climate change top many lists in terms of both likelihood and impact. This means that organizations need to be mindful of the sustainability of their investments and actions. From property loss due to extreme weather events to repuation risk due to "flight shaming," businesses must evaluate their contributions to these problems and strategize ways to demonstrate corporate responsibility.

It's no surprise that cyber risk continues to be another major risk category. Here, the emerging trend is to take cybersecurity from the server room to the board room. Solutions to cyber risk must extend beyond technology and IT experts. To be resilient, an organization must implement a cyber strategy that includes all aspects of the business, driven by governance initiatives. Organizations should conduct benchmarking studies on their current state of cyber vulnerability, proactively educate and train their entire staff in cyber hygiene and response best practices, and protect themselves with insurance policies to support response and recovery efforts in the event of a cyber incident.

Finally, the role of risk management is expanding from the protection of tangible assets to intangible ones, like data and reputation. To adequately mitigate these intangible risks, a robust Enterprise Risk Management (ERM) strategy must be in place, championed by the Board for top-down implementation, and bolstered by data-driven models and analytics techniques. This kind of holistic approach keeps new and emerging risks from remaining undetected, building readiness and resliency.

HAVE A QUESTION FOR OUR EXPERTS?

Send your inquiries to info@riskcooperative.com and your question and answer may be published in a future edition of Risk Matters.

Announcements

RISK COOPERATIVE CELBRATES 5 YEARS

On November 6, 2014, the Risk Cooperative team of risk and insurance executives founded a specialized strategy, risk and insurance advisory firm. Over the last 5 years, Risk Cooperative has been one of the fastest growing firms in the industry and has become a globally recognized leader in the fields of risk, resilience, national security and cybersecurity.

https://riskcooperative.com/timeline/

RISK COOPERATIVE ANNOUNCES EXECUTIVE APPOINTMENTS AND TRANSITIONS

As the company approached its 5th anniversary, governance changes among Risk Cooperative's co-founders were made to usher in new era of growth. Andres Franzetti, former head of strategy has served as President and Chief Operating Officer since January 2019, and will assume the role of CEO. Dante Disparte, will transition to Head of Policy and Communication for the newly formed Libra Association and will continuing his work with Risk Cooperative as its Chairman.

https://riskcooperative.com/press-releases/risk-cooperative-announces-executive-appointments-and-transitions/

HARVARD BUSINESS REVIEW: CYBER SECURITY ESSAYS

Just in time for October's cybersecurity awareness month, an article from Dante Disparte was published in the Harvard Business Review's collection of Cybersecurity essays. Cyberattacks on companies and individuals are on the rise and growing not only in number but also in ferocity. And while you may think your company has taken all the precautionary steps to prevent an attack, no individual, company, or country is safe. Cybersecurity can no longer be left exclusively to IT specialists. Improving and increasing data security practices and identifying suspicious activity is everyone's responsibility, from the boardroom to the break room.

https://store.hbr.org/product/cybersecurity-the-insights-you-need-from-harvard-business-review/10280

Risk Cooperative

LIFE & HEALTH | PROPERTY & CASUALTY | COMPREHENSIVE BENEFITS | SPECIALTY INSURANCE

Risk Cooperative, a coverholder at Lloyd's, is a specialized strategy, risk and insurance advisory firm founded around the question, what would you do in a world without risk? Risk Cooperative is a licensed brokerage across the full spectrum of risk and insurance solutions.

www.riskcooperative.com