Risk Matters

A SEMI-ANNUAL PUBLICATION | SUMMER 2019

Beyond the Numbers

High Price of Underinsurance

" If you do not change direction, you may end up where you are headed."

RC ANSWERS:
Selecting the best brokerage for your enterprise needs

In Memoriam, Our Featured Risk Leader: **Jaqueline Grapin**

SUMMER 2019

Risk Cooperative

Contents

"Playing it safe is the riskiest choice we can ever make."

COLUMNS

FEATURES

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

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

Since founding Risk Cooperative in late 2014, we have addressed the most complex issues with risk, readiness and resilience, doing so where profit and purpose are not in conflict. With this issue of Risk Matters, we mark some important transitions in our journey, without losing focus for why Risk Cooperative exists.

Somberly, we devote our featured Risk Leader profile to the memory of Jaqueline Grapin, an economist, journalist and stateswoman par excellence. When my colleagues and I founded the firm, we knew that going far meant not going alone, for which the invaluable counsel of an advisory board would not only keep us true to our mission, it would challenge us along the way. As our first advisor, Ms. Grapin was not only the most engaged, she has provided invaluable and irreplaceable advice for which we continue to benefit. I will personally miss her and Risk Cooperative will continue to observe and strive to emulate her example.

Additionally, Risk Cooperative is undergoing its own transitions as we near our 5th anniversary. As a direct result of the innovative work at Risk Cooperative, I have been asked to serve in a new role as the head of policy and communications for the newly announced Libra Association. I will continue to serve Risk Cooperative in a new role as Chairman, and am honored to hand the keys—and the pen for future editions of *Risk Matters*—to Andres Franzetti, who will replace me as CEO. Andres, along with our growing and diverse team of risk leaders, has capably run the firm as president and COO since January 2019 and as a key executive from the beginning. I have every confidence our better days lie ahead.

As our curated insights in Risk Matters have highlighted over the years, the world is facing a number of key threats to stability, stemming from man-made, natural and emerging causes. None is more insidious than issues related to financial inclusion and economic opportunity, which has left billions of people on the margins of the global economy. Addressing the root causes of these issues will be a principal focus on my new role with the Libra Association, whose mission to enable a simple global currency and financial infrastructure that empowers billions of people, which is in line with making the world more resilient.

Dante Disparte is the founder and Chairman of Risk Cooperative, and co-author of the book "Global Risk Agility and Decision Making"

Featured Risk Leader

IN MEMORIAM

Armed at the age of 24 with three master's degrees in law, business and political science, Ms. Grapin (married Le Goc) was hired by Hubert Beuve-Méry as the youngest journalist of the time at the French newspaper *Le Monde*. In charge of creating a micro-economic section, she developed a new and unique tone reporting on economic and financial information. Her innovation followed the life of European companies and their various industrial strategies. Following her widely read economic section, she contributed to the creation of the first European publication in several languages: the *Europa* supplement, published by *Le Monde* in France, *The Times* in Great Britain, *Die Welt* in Federal Germany, and *La Stampa* in Italy of which she was elected the overall editor-in-chief.

JAQUELINE GRAPIN,
FOUNDER AND CHAIRMAN,
THE EUROPEAN INSTITUTE AND
PUBLISHER OF EUROPEAN AFFAIRS

Having gained experience in European affairs (through *Europa's* editor-in-chief position), and American business (through the publication of several books and numerous articles on the United States), Ms. Grapin perceived the need for enhanced collaboration and communication between Europeans and Americans in the United States (U.S.) capital Washington D.C. at a time when the process of European integration made it necessary to have a better understanding of European integration and impact in American circles. In liaison with the Embassy of France in Washington, and with the Commission of the European Communities in Brussels, Ms. Grapin founded the European Institute in Washington in June 1989. While 23-member countries of the Community were directly involved in this initiative, as well as many European and American companies, and Washington's main think tanks, the Institute worked closely with the United States Administration, Congress, the European Commission, and the European Parliament. The development of the European Institute's programs, centered mainly on issues of economic strategy and security, aroused such interest that it quickly became respected and recognized on both sides of the Atlantic.

Her more than twenty years of experience led to developing a robust network and a quality of judgment on situations, which proved beneficial in periods when the coordination between Europe and the U.S. was difficult and where a global perspective and strategy is needed.

Ms. Grapin participated, in various capacities, in the work of global institutions such as the World Bank and the International Monetary Fund, and international non-governmental organizations such as the Aspen Institute, the International Women's Forum, International Women's Media Foundation and the International Institute for Strategic Studies, London. Furthermore, she served on the International Advisory Council of La Poste, was a member of the Advisory Council of the Kogod School of Business at American University in Washington D.C. and the Board of Directors of the Jean Monnet Foundation in Lausanne, Switzerland. Additionally, she served on the Board of Directors of the humanitarian organization Action Against Hunger (AAH-USA) in New York.

Featured Risk Leader

IN MEMORIAM

Elected President of the Association of Trade Advisers (Conseillers du Commerce Exterieure) of France in Washington D.C. in 2008, she gave this group of French business leaders residing in the United States a dynamic all the more beneficial as they worked in synergy with the Minister for Economic and Financial Affairs of France in Washington.

During the last crisis of Franco-American relations at the outbreak of the war in Iraq, and during the recent financial turmoil, thanks to her privileged relations with the State Department, the Treasury and the Departments of Commerce and Defense, Ms. Grapin maneuvered in coordination with the French Embassy in Washington D.C. to limit the damage inflicted on the Franco-American relationship. She was a permanent voice of optimism and pragmatism that was highly appreciated if judged by the tributes paid to her by ambassadors and U.S. government officials. Ms. Grapin made frequent public appearances, speaking on various aspects of European developments and U.S.-European relations. In the U.S., she was a regular guest of The NewsHour with Jim Lehrer, CNN, C-SPAN and National Public Radio.

Because of the work she has completed throughout an exceptionally rich career, she was able to contribute to the decision-making process of local businesses and communities with respect to their American and European development options as well as their business, marketing and investment choices. Supporting Risk Cooperative in its infancy stages and observing its growth proved to be the highlight of the last few years with her health deteriorating.

Recognized for her dedication to France, Ms. Grapin was a Commandeur in the French Legion of Honor, the highest French order of merit.

Ms. Grapin's optimism, charisma, and influence benefited both sides of the Atlantic. During a period where international relations appear to be at an impasse, the loss of Mrs. Grapin can be felt. Perhaps it isn't coincidence that the appeared strained transatlantic relationships manifested itself a few short months following Ms. Grapin stepping down as President of the European Institute.

Ms. Grapin is survived by her daughter Claire and son Julien. A special ceremony honoring her life will be held in the Fall of 2019 in Washington D.C.

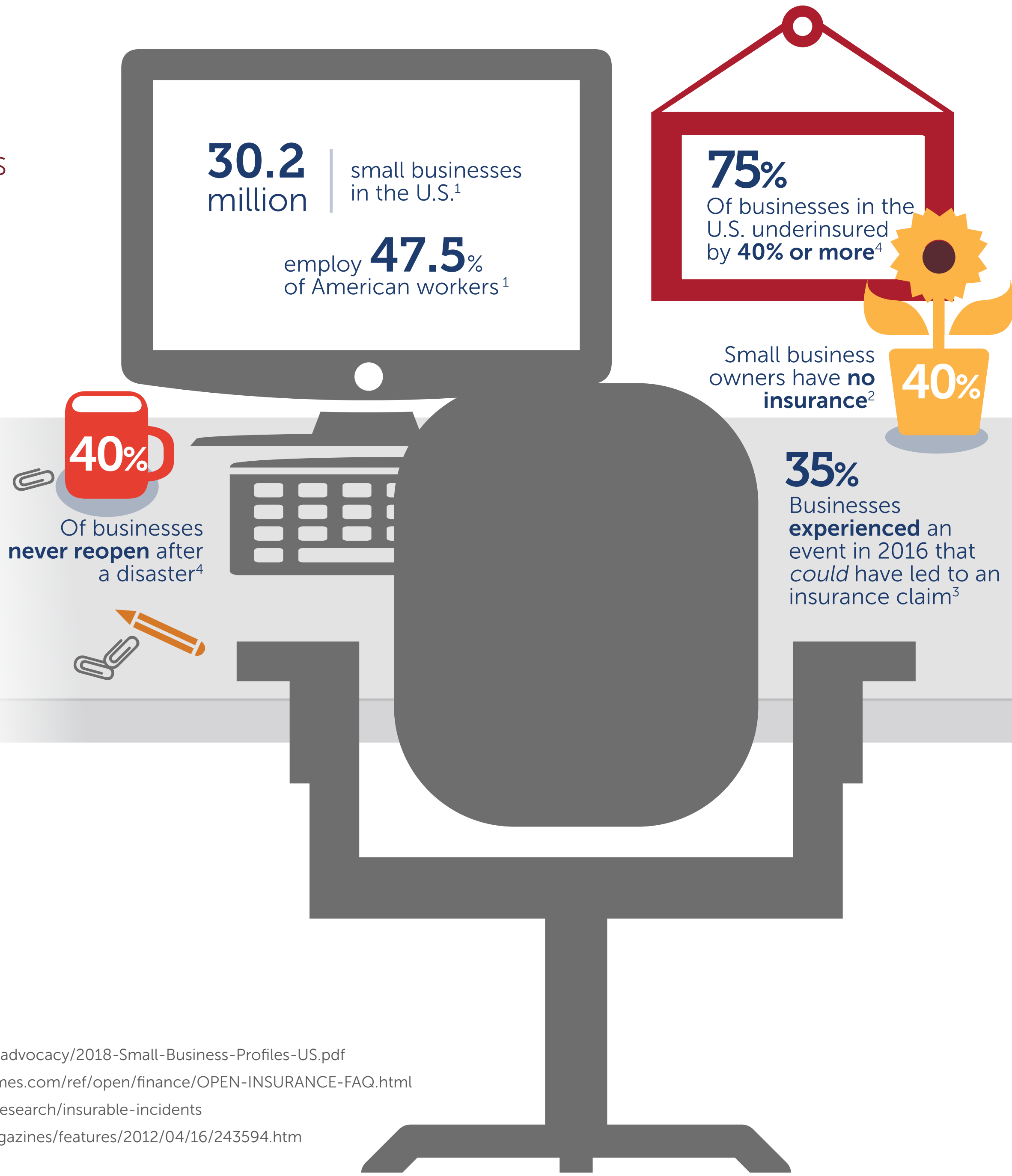
By the Numbers

THE HIGH PRICE OF UNDERINSURANCE

SMALL BUSINESSES EXPERIENCE RISK EVENTS AT HIGHER RATES THAN INSURANCE CLAIMS, EXPOSING AN **EPIDEMIC OF UNDER INSURANCE.**

MANY BUSINESSES OWNERS FEAR RISING PREMIUMS WILL RESULT FROM A CLAIM—IF THEY HAVE SECURED INSURANCE COVERAGE AT ALL.

ULTIMATELY, MANY BUSINESSES DON'T SURVIVE A DISASTER, **COSTING OWNERS AND EMPLOYEES THEIR LIVELIHOODS.**



[1] https://www.sba.gov/sites/default/files/advocacy/2018-Small-Business-Profiles-US.pdf

[2] https://archive.nytimes.com/www.nytimes.com/ref/open/finance/OPEN-INSURANCE-FAQ.html

[3] https://www.insureon.com/resources/research/insurable-incidents

[4] https://www.insurancejournal.com/magazines/features/2012/04/16/243594.htm

Summaries

NOTRE DAME WILL RISE FROM THE ASHES | PUBLISHED 04.17.19

Written by Dante Disparte
Originally published on International Policy Digest

In the Notre Dame blaze, 850 years of world heritage burned. Yet, the tragedy marks a point of national solidarity for a deeply divided French society, roiled by months of civil unrest at the hands of the gilets jaunes. While the wooden roof is all but lost, much of Notre Dame's treasures have been spared, which should spur a review of safety and emergency measures for such vital world heritage sites, that serve as powerful symbols of human ingenuity, belief and collective capacity.

Read the full article: https://intpolicydigest.org/2019/04/17/notre-dame-will-rise-from-the-ashes/

SMART DUBAI, BUILDING THE HAPPIEST CITY ON EARTH | PUBLISHED 03.09.2019

Written by Dante Disparte
Originally published on Forbes.com

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.

Read the full article: https://www.forbes.com/sites/dantedisparte/2019/03/09/forbes-exclusive-smart-dubai-building-the-happiest-city-on-earth/#11de83554753

THE BLURRED LINES OF PRIVATE WEALTH... AND HOW TO MANAGE THE RISKS | PUBLISHED 10.21.2018

Written by Dante Disparte
Originally published on Forbes.com

Protecting the wealth and assets of a millionaire or billionaire client is more akin to managing enterprise risks than personal ones. This piece explores some of the particular challenges facing the affluent, from personal security to cyber risk to the particular impact of climate change on vulnerable assets.

Read the full article: https://www.forbes.com/sites/dantedisparte/2018/10/21/the-blurred-lines-of-private-wealth-and-how-to-manage-the-risks/#5ac5c7bc7373

GOVERNMENT SHUTDOWN | JANUARY 2019

In Risk & Insurance, Les Williams offers advice on navigating healthcare coverage challenges for furloughed government contractors and the fallout for employers in the aftermath of the shutdown.

Read the full article: https://riskandinsurance.com/health-care-coverage-during-the-government-shutdown/

Dante Disparte published his thoughts on the broader economic impacts of the unprecedented shutdown on Forbes.com.

Read the full article: https://www.forbes.com/sites/dantedisparte/2019/01/11/the-longest-u-s-government-shutdown/#6ac27c3069e5

Featured Analysis

DID IBM JUST BREAK BLOCKCHAIN?
| PUBLISHED 01.19.2019

Written by Dante Disparte
Originally published on Forbes.com

Crypto winter, which has produced a massive market correction on bitcoin and other cryptocurrency prices, may now extend the big chill on blockchain as well. Beyond the rather convenient management consulting dismissals that blockchain hype has slipped into the valley of disillusionment, the world's most resilient technology may face its first serious technological challenge with IBM's announcement of commercially ready quantum computing.

While blockchain and distributed ledger technologies come in many shapes and sizes, proponents of the bitcoin blockchain and other public ledgers have long advocated for the property of resilience by design. Some going as far as claiming that the bitcoin blockchain is unhackable by today's technological standards, due in no small measure to the distributed, encrypted and consensus-driven mechanisms that require broad agreement among many systems to ledger a transaction. This "hardened" posture of blockchain has up until now and by today's technological standards proven to be very resilient indeed. One study claimed that to hack the bitcoin blockchain was as likely as winning the Powerball lottery 9 times consecutively. Those odds, which no betting person would wager on, have just received a considerable challenge with the advent commercially viable quantum competing as IBM introduces the first generation of the IBM Q System One – the q standing for qubit, which is the basic unit of quantum information.

The claims that true blockchains are unhackable or the more accurate designation hack resistant negates the reality that complex systems fail in complex ways. This much is true especially when you countenance an evolving cyber risk landscape that is propelled by Moore's law, as much as the miniaturization and commercialization of quantum computing is now a market reality – and several years ahead of schedule at that. Does this mean that blockchain is immediately more vulnerable and that people's crypto hoards now face an additional peril beyond the ever-present risks in the space? The answer is a cautious no, at least for now.

Any would-be exploit of true blockchains or a large-scale crypto heist exploiting quantum computing, despite IBM's announcement, can only be carried out by a nation state actor or a very determined enterprise with deep pockets and a lot of physical space. The 9 by 9 tower encasing IBM's quantum computer hearkens to the mainframes of the early days of computing, which filled entire rooms. But as a first foray into the democratization of quantum computing, IBM has made a considerable first move. This first version will of course continue to evolve apace with technological advancements and market adoption, which will then imply further miniaturization and, hence, proliferation of the computing power necessary to fall into nefarious hands. When this occurs, which may be as soon as 2020, true blockchain projects and large crypto nest eggs in the hands of even the most cyber mature digital asset custodians may face a hitherto unimaginable peril.

Just as 51% attacks where once considered improbable, the prospect of quantum computing power being arrayed against blockchain and the valuable treasures and truths they hold have now entered the realm of possibility, albeit remote. Blockchain technology, like cloud computing or that other foundational technology the internet

Featured Analysis

before it, is very much in its infancy, despite bitcoin's tenth anniversary. Serious players, including IBM and other technology majors, are also evolving with blockchain and, critically, their management understanding of the underlying technology and how it can impact core functions of their business and the economy overall. To this end, blockchain's evolution, efficiency and security are also not constants, but evolving at the rate of technology innovation as well.

One crucial item to remember about blockchain, like all other technologies in the digital transformation toolbox, is that it is not to be used in isolation or as a constant, no matter how permanent data may be on its records. Like the migration to cloud computing, which is a largely uninsured and risk-prone option, blockchain and advanced technologies are infinitely better and safer than many of the legacy, honey pot systems and databases used today. These very legacy systems are easily broken by low-cost high-impact social engineering, phishing and targeted whaling scams, cyber extortion and comparatively unsophisticated ransomware attacks that do not require millions spent on quantum computing. So, despite IBM's impressive foray into leveling the quantum computing playing field, blockchain advocates and digital change leaders need not worry for now. They likely face greater risk from project selection and execution in educating their board rooms than from technological vulnerabilities.

https://www.forbes.com/sites/dantedisparte/2019/01/09/did-ibm-just-break-blockchain/#71ad58c94c6f

---

ELON MUSK VERSUS THE SEC: WHEN A TWEET COSTS $40 MILLION | PUBLISHED 09.29.2018

Written by Dante Disparte
Originally published on Forbes.com

Elon Musk, Tesla's crestfallen chairman and CEO, is arguably a controversial leader. At once heralded as the type of prolific entrepreneur and visionary for whom space and the internal combustion engine are not complex obstacles, but rather the next frontier for his companies, SpaceX and Tesla. To others, however, he is the very emblem of erratic corporate leadership, marking the limits of imagination, personal restraint and hyper-productivity, even suffering from what some would call an Icarus complex, with one wax wing a Twitter account and the other hubris.

Elon Musk has not only flown to close to the sun, he has perhaps Tweeted all too often under the twin guise of impetuousness and imperviousness, which resulted in a $20 million settlement with the Securities and Exchange Commission, SEC, for which he is personally liable. This also comes with an agreement that he would step down as Tesla's chairman in 45 days. Separately, Tesla has agreed to pay $20 million to settle claims that it failed to put up guardrails on Elon Musk's communications, which may be an impossibility, along with the addition of two independent directors to replace Elon Musk on the company's 9-person board, which includes his brother. All of this conspires to show that micro-sized communications, 280 characters at a time, can be costly indeed with outsized effects. The words of that other prolific inventor Benjamin Franklin spring to mind when he said a slip of the foot you may soon recover, but a slip of the tongue you may never get over. A timeless aphorism that could have spared Tesla shareholders the 30% freefall from the August 7, 2018 share price of $379.57 to the September 28, 2018 close of $264.77, along with the expected wild ride that lies ahead.

In many ways Elon Musk dodged a bullet, for the SEC's original lawsuit carried the heftier punishment of banning him from serving as a public company director or officer. This would have been a veritable scarlet letter for such a prolific leader and an example to Musk's supporters of an excessively punitive action. How the market, and perhaps most tellingly Tesla's board, responds to these costly settlements remains to be seen. More importantly, with a $40 million tweet, a mere rounding error of Musk's $19.7 billion net worth and Tesla's $50 billion market cap, what will the board and investors demand of Elon Musk? The punctuation mark that ended Musk's summer of discontent was the ill-fated tweet on August 7 suggesting that he had arranged the capital to take Tesla private at $420 a share, something that was later posited as a Saudi-backed deal, but turned out to be a marijuana reference to amuse his girlfriend. As it happens, no such deal was in hand, shareholders where left scorned, the SEC's enforcement units were alerted and, ironically and perhaps unrelatedly, the Saudi's invested $1 billion in Lucid, a Tesla competitor. This cascade of errors, for which a tweet was the closest proximate cause, is a painful example of unintended consequences.

While this is clearly one of the costliest Tweets Elon Musk – or perhaps anyone – ever issued, it is not the most erratic, which risks adding to Musk's potential disrepute as it shows a CEO who has his eye off the ball. During the drama that unfolded in Thailand to rescue 12 wayward soccer players and their coach from a flooded cave, Elon Musk got into a Twitter-tiff with Vernon Unsworth, a British diver, over the rejected mini-submarine Tesla engineered in a bid to aid rescue efforts. While the miraculous rescue of the boys and their coach should have been the end of the story insofar as it involves Elon Musk, the companies he leads or the shareholders and stakeholders who entrust him, this case descended into a bizarre series of Twitter accusations made by Elon Musk that Vernon Unsworth was a pedophile. An accusation that has resulted in further legal action. All of this is clearly an unnecessary distraction and while $40 million will hardly register on Elon Musk's or Tesla's financial accounts, it does add to legitimate concerns about strategic and operational distractions.

These distractions include the loss of key executives, the loss of potential privatization suitors, to the extent Saudi courtship was legitimate, as well as very real customer product liability, quality and safety concerns, that now include a 19-month Model 3 backlog. When you build an iconoclastic product like a Tesla vehicle, that at once breaks the carbon-hungry dependency on fossil fuels and the century-long monopoly of the internal combustion engine, while bridging a technologically ludicrous hands-free future, there are bound to be risks. While a Tesla driver may occasionally let go of the wheel and can be distracted at their own peril, there is a much higher standard for those at the helm of publicly-held companies.

https://www.forbes.com/sites/dantedisparte/2018/09/29/elon-musk-versus-the-sec-when-a-tweet-costs-40-million/#52a140761556

Featured Analysis

WHY MORE EMPLOYEES ARE GOING THE 1099 ROUTE AND OTHER INSIGHTS FROM A VETERAN RISK MANAGER | PUBLISHED 04.15.2019

Profile of Les Williams
Originally published on Risk & Insurance

Risk Insider Les Williams, partner and chief revenue officer of Risk Cooperative, recently shared his insights on some of the top challenges facing the insurance industry today, from talent recruitment and retention to resiliency against emerging threats posed by climate change, weakening infrastructure and IoT vulnerabilities.

R&I: You've written about the risks facing employers regarding talent recruitment and retention. Given the burgeoning "gig economy" and increasing reliance on automation, what does the workforce of the future look like?

Les Williams: A lot of our clients have trouble holding on to technology workers, especially millennials, because in the gig economy people have more options. They want to be able to work virtually as needed. We are seeing more transient folks who will switch jobs more frequently because there's so much opportunity out there.

More employees are going the 1099 route, especially tech workers. They don't want to be a W-2 employee; they want to be more in control of their own time, so they're forming their own LLCs and working as freelancers full time.

That can be a gift for employers. You don't have to pay for their health insurance, for one thing, and you can more easily fill positions that have high turnover. But you may also have to increase policy limits for some things. Crime, for example. You're sharing more information and access with outside workers, and you run a higher risk because you don't really know these folks and can't vet them as well as you might an internal employee.

R&I: So what are some strategies for employers who want to hold on to their talent?

LW: One of the interesting things we've seen in our research at Risk Cooperative is how much health is becoming a fashion statement for younger workers. Having a new, reusable water bottle is as much a fashion accessory as having the latest iPhone. Health is the new wealth.

As a result, more companies are putting employee wellness programs in place. So workers can accrue points for things like taking yoga classes or drinking a certain amount of water every day and redeem their points for rewards like gift cards. There's an element of gamification to it.

There's one company called SoHookd that bills itself as a "wellness-based loyalty platform." They built an online marketplace where users can redeem points for things like fitness classes, organic groceries, massages. Younger workers would rather receive these experiential rewards in the form of a health-conscious object rather than a monetary reward.

R&I: What about insurance and risk management specifically? What would you tell a college graduate about the industry to get them interested?

LW: When I'm on a plane and I don't want to talk anybody, I tell them I'm an insurance broker. But when I want to have a deep conversation, I tell them I'm a risk manager.

Risk management is about putting processes in place to solve a problem. Risk management is complex; is not surface level. There's a lot of technology involved and a lot of engineering involved. That's usually the piece that gets younger people interested.

When people hear I work in insurance, they think I'm going to talk to them about bundling their home and auto, but when I describe what really goes into risk management, they see how varied and interesting it can be, and how futuristic it can be.

Technology is becoming the backbone of risk management.

R&I: You have a varied background yourself, with a degree in mechanical engineering, an MBA, and a host of roles in business development. What attracted you to risk management?

LW: Engineers, like risk managers, are problem solvers. I've always loved solving problems. At Ford Motor Co., my first job, one of my first responsibilities was trying to figure out why a vehicle was stalling. There's a thousand of reasons why a vehicle could stall.

We found the answer was heavy key chains. The ignition switch was supporting all of the weight, so when the car drove over a bump, the heavy key chain would pull down the ignition and turn to the off position. So we had to find a way to remove the pressure and make ignition switches more robust so stalling wouldn't happen. That's risk management.

At IBM, I managed a team of 12 salespeople, and we were getting complaints from customers who were receiving multiple calls from different team members. We didn't appear too organized. So I had to reorganize my 12-person team so they would do a better job of communicating with one another to prevent clients from getting upset and leaving. That's risk management.

When I worked in commercial real estate at JLL, I had clients who needed help finding office space, and they always underestimate their future growth. So I would suggest looking at another building that wasn't as well-leased so two years down the line we don't have go through this process again.

Risk management is putting processes in place so things don't go wrong. All the different jobs I've had were doing that, just in different ways.

R&I: What do you see as the most concerning emerging commercial risks?

LW: There are three that are connected: aging infrastructure, climate change and cyber risk in the Internet of Things.

Back in 2017, the American Society of Civil engineers gave America's inland waters a D score. Much of the waterway infrastructure hasn't been updated since the 1950s. We saw the impact of that recently in Nebraska, Iowa and Missouri, where rising flood waters left large areas completely submerged. Repairs take time; days or sometimes weeks. Delays at some of the locks in some of the rivers have doubled. That has impacts for the supply chain.

Climate change is intertwined in that. Currently, we're 1 degree Celsius warmer than in pre-industrial times. Drier seasons are exacerbated. Rainy seasons are exacerbated. Weather is more severe and our infrastructure just can't take it.

Featured Analysis

As far as cyber and the IoT — by 2020 there will be about 20.4 billion interconnected devices globally. As much as 37 percent of those will be used outside of consumer settings. Connected equipment will play a role in our infrastructure — monitoring dam openings, the electrical power supply, etc. What's scary about that is that bad actors can hack into those systems and cause havoc.

We already have evidence that our electrical grid has been hacked.

Globally, cyber job demand is going to outpace supply by about 1.8 million jobs by 2022. So at the same time a lot of our critical infrastructure is exposed, we won't have the workers to help protect it. All of these were detailed in the World Economic Forum's recent global risks report.

R&I: What can the industry do to mitigate these risks?

LW: Insurers have a lot of influence. They have the power to say, 'we're not going to provide insurance for your building if it's not resilient enough to withstand a flood.' Or strong winds, or hail, or whatever the hazard may be in that region.

Insurers have to put their foot down and say, 'if you want to have this entity, these are the risk management protocols that must be in place to get covered.' I think we will see carriers starting to take a stronger stance.

Insurers can also lobby for more money being spent on sustainability projects.

The EPA invited almost 40 projects in 16 states to apply for loans under the Water Infrastructure Finance and Innovation Act. There's an available $5 billion in funding to help finance water infrastructure projects. Insurers can encourage private companies to invest in infrastructure projects as well, bringing private sector capital off the sidelines.

Not only is this the right thing to do for society, it will also help to reduce catastrophic claims.

https://riskandinsurance.com/les-williams/

VIRULENT RANSOMWARE STRAINS TRUST IN CYBER INSURANCE | PUBLISHED 03.04.2019

Written by Dante Disparte and Andres Franzetti
Originally published in International Policy Digest

While the threat of ransomware has been around for a while, new more potent strains of this attack vector have emerged. From the May 2017 WannaCry dragnet, which held computer systems for ransom in more than 150 countries – all executed at blinding speed over a weekend – to the NotPetya attack on June 27, 2017, which wreaked havoc on many large companies, including the Danish shipping giant Maersk, which incurred an eye-watering $250 to $300 million in costs, to the more recent ransomware attack on the city of Atlanta, which successfully brought critical services in the city to a standstill, it is clear that attacks have grown more complex and motivations broader. Indeed, the newest cyber monster to hit the scene is the aptly named LockerGoga, which has successfully crippled industrial system. While the origination and economic demands of each of these attacks may be different, they all invariably point to the growing cyber insurance market as a possible line of financial defense and remediation. Trust in this market is under strain due to high-profile claim denials.

Herein, the fact that insurance is little more than a promissory statement outlining coverage, exclusions and conditions are being laid bare and straining trust in this financial instrument, which is used to operating in black and white or binary claims scenarios. Cyber threats, by their very nature, are not only amorphous, but they are also extra-territorial and often lay dormant in a company's systems for years undetected. Indeed, the average computer exploit goes undetected for an average of 206 days, often creating a veritable back-door into company or, worse yet, state secrets. This complex and hard to track risk landscape is prompting national security officials and public policy leaders to call for a complete overall of third-party and supply chain operating standards when it comes to cyber threats.

Against this measure, the Pentagon promises to roll out new operating parameters for government contractors and their first and second tier supply chain partners, on whom not only access to systems but critical data, is a requisite of their work. Operating on a one-size fits all approach from a standards point of view is one thing, which over time can drive improvements in cyber-hygiene, notwithstanding the risk that self-reporting on adherence can create. The backstop for these approaches, especially if cracks begin to emerge is the cyber insurance market, which can help companies shore up their financial war chest (or lack thereof) for cyber threats, compliance costs, and remediation, tapping a veritable digital fire brigade that many of the insurers have on call. This class of insurance is not only the fastest growing, with year over year growth rates of 33.8% projected between 2019 and 2024. In an industry that has taken many profit hits due to headwinds in the market and a volley of catastrophic losses, potentially risky bets on cyber insurance, especially for bundled policies, may prove to be a foolhardy exercise in hindsight. This is especially true given the hidden or systemic nature of cyber risk, for which many insurers are tacitly on the hook.

Large systemic claims courtesy of this new breed of sophisticated cyber-attacks is demonstrating the relative immaturity of the cyber insurance market, as well as the growing likelihood of catastrophic losses, which have been underfunded due to overly optimistic actuarial models, along with low

Featured Analysis

penetration in key market segments. That WannaCry only yielded a pittance in ransom monies, netting approximately $300 per attack and total global losses of $100 million in bitcoin, does not mean the threat was not a potentially cataclysmic near-miss, hitting all the insurers in the 150-country dragnet all at once with the same type of claim. Herein, the "devil's in the details" nature of insurance policy language has come to the forefront, as Mondelez, the Swiss-based firm, and owner of the Oreo cookies brand, takes on Zurich over its $100 million denial of a cyber claim arising from NotPetya. While the case is playing out, the defense argument largely hinges on the issue that NotPetya, suspected to have emanated from Russia, was, in fact, a war risk, triggering policy exclusions against force majeure claims.

Similarly, DLA Piper, one of the world's largest law firms is fighting a similar claim denial in the UK over the very same ransomware event as Zurich, in this case embroiling Lloyd's insurer Hiscox. Insurers generally take pride in their claim's performance, especially for comparatively new classes of insurance, as this is a way of creating market proof that coverage works. While these types of cases are complicated, especially as cyber insurance cannot be viewed in isolation of other insurance policies in force or the contributory causes of an event, these types of examples are giving pause to the industry, while raising questions among insurance buyers about the efficacy of these programs. At the core, other than balance sheet prowess, insurance companies writing cyber risk aim to gain marginal differentiation at the policy language level and on what constitutes a covered peril. With ransomware, whose origins, motives and latency are difficult if not impossible to forensically trace back to its source, a force majeure or war risk exclusion could theoretically remain an industry ambiguity, eroding confidence in the sector and the insurance class writ large.

Additionally, the systemic nature of this risk, and aggregation issues of insurers exposed on multiple fronts to cyber risk, compounded with the impacts to smaller firm's survival rates after a cyber-attack, a black swan scenario starts taking shape. A recent Lloyd's study looked at this very scenario, examining the economic impacts of a large-scale cyber-attack taking down a cloud service provider. Their findings demonstrated that a cyber incident that takes a top three cloud provider offline in the U.S. for 3-6 days would result in loss estimates between $6.9 and $14.7 billion and between $1.5 and $2.8 billion in industry insured losses. When further examining the effect on smaller companies, who may be more likely to utilize cloud providers to avoid expensive infrastructure costs but are also more reluctant to take up cyber insurance, the repercussions and loss of confidence from these types of exclusionary languages becomes more problematic. Cybercriminals are known to prey on small to midsize firms as easy targets, and according to the National Cyber Security Alliance, 60% of small and midsized businesses that suffer a cyber-attack, go out of business within 6 months. With approximately 26 million small and midsize business in the U.S., the economic impact of a mass cyber-attack and corresponding insurance impacts would be far worse than the financial crisis of 2008 where a total of 800,000 businesses closed their doors over a prolonged period. The sum of these firms create a massive potential attack surface area and many of the providers they rely on, such as payroll providers, like ADP, may very well be systemic firms hiding in plain sight.

For these reasons, we have long advocated for a backstop against potentially catastrophic cyber events, as well as harmonization particularly among small to mid-sized enterprises, the weakest links in an economy or a supply chain, akin to the FDIC. The erosion of confidence in any one bank erodes confidence in banking. It would stand to reason then, that the emergence of high-profile, high dollar cyber claim denials potentially imperils confidence in this aspect of the insurance industry. While cyber insurance is fast growing, the adoption of stand-alone cyber insurance, which would respond to a covered claim on a first-dollar basis, remains low at 16% in the U.S. The remainder of the market, comprised of "Frankenstein" or hybrid policies that bundle some nominal form of cyber protection, low dollar amounts, and circumscribed coverage adds to market confusion, particularly among customers that do not hold personally identifiable (PII) records.

To the firm that treats cyber threats as merely a privacy and compliance driven risk, the business continuity lessons courtesy of this damaging new breed of ransomware attacks, which have moved down market to so-called "soft targets" should serve as a wake-up call. Cyber risk is first and foremost a business continuity issue, for which the speed of response, the scope of coverage and prevention are the best cures. If cyber insurers want to continue enjoying market confidence for this class of insurance, they would be well-advised to form a consensus on what constitutes a covered claim and ensure their customers, brokers, and agents know precisely what they are trading in.

https://intpolicydigest.org/2019/04/03/virulent-ransomware-strains-trust-in-cyber-insurance/

ORACLE: ON THE WORLD'S DATA LAKE, A BLOCKCHAIN SWAN | PUBLISHED 02.28.2019

Written by Dante Disparte
Originally published on Forbes.com

With a tempering of blockchain fanfare as the technology crested the peak of the hype cycle, Oracle's two-year-old foray into the blockchain domain may have gone largely unnoticed. Especially as it might have been dismissed as a copy cat or catch up move, as yet another large technology firm converted to the blockchain gospel like Microsoft and IBM before it. Oracle's move, however, comes with a very different asset base, for which it is starting to realize gains from its blockchain offering. If the wellspring of all digital transformation is an enterprise's data lake and how it connects across markets and stakeholders, then Oracle, the world's largest database provider with number one positions in virtually every industry, has not only built these reservoirs, its software and more than 137,000 employees serve as the access channels to the insights, markets and opportunities it holds. For this alone, Oracle may be the firm to watch and even the firm to beat as the enterprise blockchain wars heat up.

From speaking to senior leaders at Oracle, the firm knows that this broad cross-industry integration is the source of its advantage vis-à-vis its peers. How it has positioned its blockchain bet comes with a keen awareness that this next wave of technology innovation is not about discrete yet disconnected pilot projects in single industry silos. Rather, the future for enterprise blockchain efforts, especially in mature sectors, lies in making high-trust, low-friction connections between trading counterparties, wherein blockchain becomes

Featured Analysis

not only the ledger of reference, it becomes a source for entirely new operating models. Even JP Morgan's about face on cryptocurrencies with the launch of the JPM Coin, has much less to do with a free-floating speculative digital asset and more to do with counterparty trading and settlement efficiencies in the bank and with the bank's external stakeholders. One of Oracle's successful projects deployed for a mid-sized bank, helped improve the speed, security and reliability of cross-border money transfers using its blockchain solution.

This move, much like the sectors where Oracle is seeing traction, such as retail, supply chain management, money transfer, among others, is a drive to increase speed, track and trace capabilities and, critically, accelerate financial settlements between counterparties – a process that without blockchain losses billions each year to insidious sources of friction, such as one-sided bookkeeping, asymmetrical information, and financial amnesia of the deliberate and accidental variety. Because of this long-standing source of friction, all facets of the global economy and how large firms trade with each other is a highly audited, costly and untrusting operating environment. Overcoming this burden of proof leads to low levels of customer satisfaction, slow processing times and ultimately high costs of evidencing rightful claims. Indeed, another successful Oracle blockchain deployment was able to collapse the time, speed and security of commercial invoicing for one of its customers.

In this word, where no one trusts each other, a would-be claimant to an insurance policy, for example, must first "decriminalize" their rightful claim to any money, a process that is cumbersome and can take years, for lingering fears of fraud and other financial risks. Imagine an alternate world where everyone participating in a commercial relationship was trusted from the outset and due commerce could flow in a highly traceable and nearly instantaneous settlement process. Oracle sits astride the data sets across industries to begin making these types of meaningful connections a reality, wherein the lack of commercial trust is the stranded asset that is being monetized. Critically, for this to work, boards and senior executives have tired of hearing about the art of the possible with blockchain, with very little in the way of real world or tangible results. To this end, Oracle has opted for a plug and play approach with the technology interface, which may be the very best way to get the technology and all the jargon to fade to the background. Like people, executive teams and boards care about outcomes and not necessarily how all the moving parts come together.

Prior to firms like Oracle and its peers entering the blockchain race with cloud-based, inter-operable and plug and play solutions, firms interested in tinkering with this emerging technology had to overcome a number of challenges. Not least of which is the general lack of technical talent proficient in coding with the various blockchain standards. The other major obstacles to enterprise blockchain adoption are the very real legal concerns voiced by legal teams about the perils of smart contracts, public data storage, notwithstanding encryption and a general managerial misunderstanding of how and where blockchain is best deployed. The relative operational immaturity and lack of cyber risk standards in the more imaginative blockchain startup ecosystem, with the QuadrigaCX scandal being a teachable moment, has done enterprise blockchain adoption few favors, as the pioneering technology gets unfairly linked to its cryptocurrency cousins. Firms like Oracle and the other enterprise blockchain majors, which already boast of a number of large-scale, real world blockchain deployments are driving an important wedge between the hype of this technology and its transformation impact.

Amid so much risk aversion with digital transformation and growing ambivalence of blockchain hype, Oracle's moves to simplify outcomes through a cloud-based, plug and play solution that sits astride its broad database capabilities can deliver that elusive return on technology investments that is so hard for mature industries to grasp. The real challenge, now that the technology stack is beginning to fade to the background, is for senior leaders to embrace new strategic thinking about the directions the markets want their businesses to go and the gains in trust they can make when they opt for decentralization in corners of their operating model. Rather than relegating blockchain to a backoffice tool in the search for marginal cost or efficiency improvements, as some industries have done, the emergence of a competitive enterprise blockchain field can embolden companies to think creatively and act decisively in their experimentation.

https://www.forbes.com/sites/dantedisparte/2019/02/28/oracle-on-the-worlds-data-lake-a-blockchain-swan/#19cb11652763

TO BLOCKCHAIN OR NOT TO BLOCKCHAIN | PUBLISHED 11.12.2018

Written by Dante Disparte
Originally published on Forbes.com

Many would argue that the enthusiasm for blockchain and cryptocurrency is waning. Indeed, according to Gartner's hype cycle, blockchain is tumbling into the trough of disillusionment where the fleet of Lamborghini's belonging to early crypto speculators have all but run out of fuel as cryptocurrency prices stabilize and regulators tighten their scrutiny of security-issues masking as initial coin offerings (ICOs) or newfangled ways of getting rich quick. If peak crypto is behind us and the blockchain bubble has burst, where does the promise of this world-changing technology go from here? Time to pack it up or time to reformulate how we think about this technology and the implied digital transformation it necessitates? Will blockchain go the way of early electric car prototypes only to lay dormant for 40 years before a Tesla comes along? Will cloud-based spreadsheets masquerading as blockchains temper enthusiasm for the value of technology investments? Many questions remain, but one thing is certain, fully harnessing blockchain has less to do with technology and more to do with advances in management thought and the art of the possible.

The argument that the blockchain bubble has burst made vociferously by the likes of Nouriel Roubini in a Senate hearing, misses a couple of key points. The first and foremost being that the technology has only come out of beta in 2017, despite bitcoin and its underlying public blockchain turning 10 this year. Since, in addition to the pilot projects being carried out by the 50 largest companies in the world (with some industries opting for "coopetition"), there

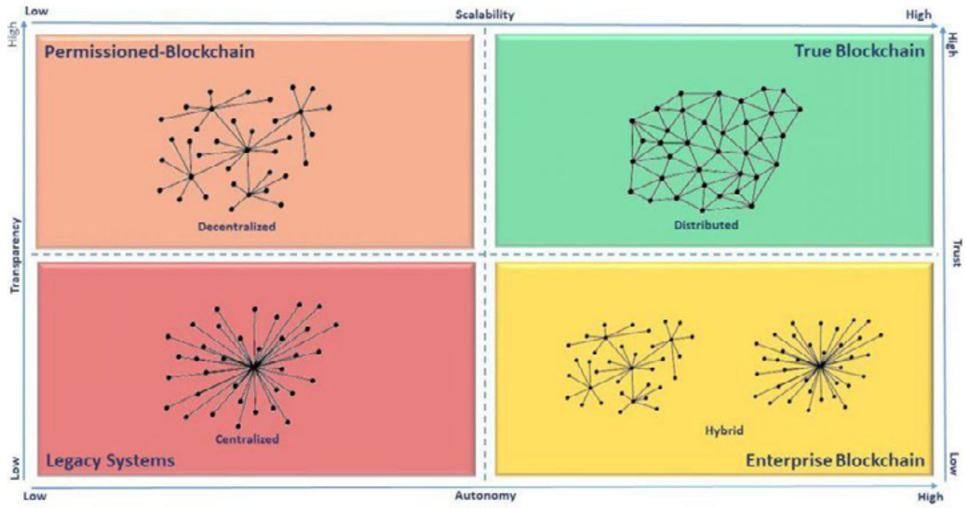
Featured Analysis

is a growing cadre of blockchain-based projects gaining serious global recognition for their potential to change the fundamental nature for how economies and essential services are organized. Unlike the internet, which is a disruptive technology borrowing from Clayton Christensen's thinking on disruptive innovation, blockchain is very much an augmenting technology. For this power to be unlocked, however, companies, entrepreneurs, technologists and policymakers need to do the unthinkable – relinquish control. This much is demanded by the market and the constituent parts of the global economy that have been telling us one thing in increasingly louder voices, they do not trust status quo or the traditional centralized structures that gain the most from it.

Implied in decentralized and distributed systems, where each node or participant operates pari passu or on equal footing, is that no one counterparty has control or more authority than another. This is a difficult and perhaps impossible level of abstraction in our current economic order, where an embarrassment of riches and power has been amassed by centralized structures, technologies and control. Indeed, the reason the U.S. Securities and Exchange Commission, SEC, is favorable toward bitcoin is precisely because of its decentralization. Is there a realm in which firms deploying blockchain can create a new category of service or solution where control, trust and value become evenly distributed? Why not! In order to get there, however, the change is not singularly about digital transformation for which blockchain cannot operate in a vacuum of other frontier technologies, it has more to do with the evolution of management thinking and organizational design. The matrix below provides a useful guide for how this transformational journey begins and where it should end in a proverbial blockchain "magic quadrant," provided project sponsors wish to fully leverage a high-trust, low-friction platform.

Against this methodology, it is difficult to identify another true blockchain project other than bitcoin, that category defying digital asset, that meets these criteria in balance. Even the crypto wunderkind Vitalik Buterin's cryptocurrency, ether, began life as a semi-centralized instrument. What does this say about the current state of play and the projects, ICOs and other supposedly world-changing applications of this technology, from digital identity, payments, supply chain provenance, even e-voting, are they blockchains at all? Or is the rate of innovation and tinkering taking place with this new technology just now getting serious, hence the accelerated appearance and demise of projects? Blockchain, like the early days of the internet, is in its thousand flowers blooming phase. The market picks winners, technologists are merely the gardeners. Some may be disappointed to learn that the path to becoming a blockchain billionaire may be harder than the one charted by the internet tech titans before them, in no small measure because of the span of control issues posed by true blockchain projects.

Much like the advent of cloud computing or the flight of imagination needed for an untethered internet, the shift to digital transformation using blockchain is more about management culture and leadership than it is about technology or informational architecture. In many ways, the technology is the easy part. The hard part is the suspension of disbelief and long-held norms about organizational approaches to trust, transparency, intermediation, control and value capture, which all conspire to form the high-friction market we currently operate in. The outcomes in this low-trust, high-friction analog world leave a lot to be expected. Billions of people are left on the sidelines without a universally portable and secure personal identity. Millions of votes are uncast, uncounted or disputed because there is no scalable high-fidelity way of addressing micro-counting and election security. Trillions in stranded assets and complex global threats are on the margins of being economically viable because current distribution, pricing and service structures make market entry unpalatable and uncompetitive. Blockchain as a technology can abundantly address these gaps. The scarcest resource appears to be the lack of imagination and will from entrenched power structures that gain the most from status quo.



A MATRIX SHOWING THE DOMAIN OF TRUE HIGH-TRUST, LOW-FRICTION STRUCTURES.

Progress with blockchain, even for large incumbent companies or power structures, need not be a zero-sum proposition. Indeed, blockchain is an augmenting technology precisely because it does not have to disrupt the type of value derived from existing systems, rather it can help create entirely new service, product and relationship models with and between markets or constituents. As an example, imagine the evolution of insurance distribution from the agent and broker-based distribution model that was borne from the analog days, to the advent of models like Geico direct courtesy of the internet, to something more akin to a customer mutual where dividends, losses and trust are managed in lockstep for a market or risk-sharing pool. Similarly, in California's move to solar-enable its housing stock by 2020, the advent of blockchain-based microgrids can ensure that older homes can buy excess energy in economical ways producing a more resilient energy matrix. Absent blockchain and management acceptance of distributed systems, which can record trust with the fidelity and permanence as an atomic clock records time, this new class of market offering would not be possible, and the assets stranded on the sidelines of the market by stubborn friction and sclerotic structures would not be activated. The question is not whether to blockchain or not to blockchain, the real question is how.

https://www.forbes.com/sites/dantedisparte/2018/11/12/to-blockchain-or-not-to-blockchain/#1b1caaa773cb

RC Answers

Insurance is complicated.
How do I select a brokerage to help me manage my needs?

Insurance can be a daunting task, especially for those outside of the industry. Identifying the right broker to help navigate the complexities of insurance policies and coverage requirements is key for any business, but particularly for smaller firms that may not have the financial resiliency to withstand a large loss. The U.S. insurance industry includes more than 825 brokers[1], so finding the right partner for your organization can be challenging. So, what should you look for in a broker?

When seeking out a broker, organizations should be looking for firms that have broad risk management experience and can provide guidance not only about the basic coverage your firm needs, but also industry trends and lesser knowns risks.

The best brokerage firms will provide a consultative approach to fully understand an organizations operation, their strategic objectives, and then develop a recommended insurance and risk mitigation approach the fits the specific client. Many brokers simply provide transactional services and "off the shelf" products that leave an organization with significant coverage gaps or underinsured due to a lack of understanding of their business.

Asking for an initial consultation before making a final decision is highly recommended. Most firms will be more than happy to offer you a complimentary review of your current insurance coverage, identifying areas for savings, ensuring adequate coverage, and potentially even unearthing coverage gaps or errors.

When contemplating to change brokers, or get second opinions, the best time to do so is 60 to 90 days before your annual renewal date. With approximately 40% of small businesses having no insurance at all, and up to 75% significantly under-insured[2], it is critical that organizations seek out qualified advice from trusted and experienced insurance advisors to ensure their organizations can withstand any potential risk.

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.

[1]According to the Insurance Information Industry

[2]Statistic from SCORE cited in Insurance Journal

Announcements

RISK COOPERATIVE LAUNCHES REMIT INSURE

RC Labs has launched Remit Insure, a product for individuals to purchase insurance that protects their financial remittances to their home countries. Given that global flows of remittances exceed $630 billion annually, remittances are vitally important. For some countries, these peer-to-peer cash transfers have comprised nearly 40% of the gross domestic product (GDP). Within the U.S., a growing population of 40 million legal immigrants and expatriates send more than $60 billion in outbound transfers each year, making it the largest sender market in the world.
excellence.

RISK COOPERATIVE AND RCM&D LAUNCH REIMAGINED PRIVATE CLIENT PRACTICE

The lines between risk and reward have blurred, as have the lines between private wealth and enterprise or portfolio value. RCM&D and Risk Cooperative have partnered to offer a reimagined private client experience that brings a comprehensive advisory, risk management and risk transfer capability to high net worth individuals, family offices, executive teams and investment funds.

RISK COOPERATIVE ANNOUNCES EXECUTIVE APPOINTMENTS AND TRANSITIONS

Governance changes among Risk Cooperative's co-founders will usher in new era of growth as the company approaches its 5th anniversary. Andres Franzetti, former head of strategy has served as President and Chief Operating Officer sice 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. Noah Skillin will serve as the company's Chief Risk Officer, responsible for overall enterprise risk management, and Les Williams will continue to serve as the company's Chief Revenue Officer leading overall sales and channel strategy. Jenny Decker has joined the team as Director of Marketing. This new structure positions Risk Cooperative for continued growth and operational excellence in 2019 and beyond.

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