Risk Matters

A SEMI-ANNUAL PUBLICATION | FALL 2017

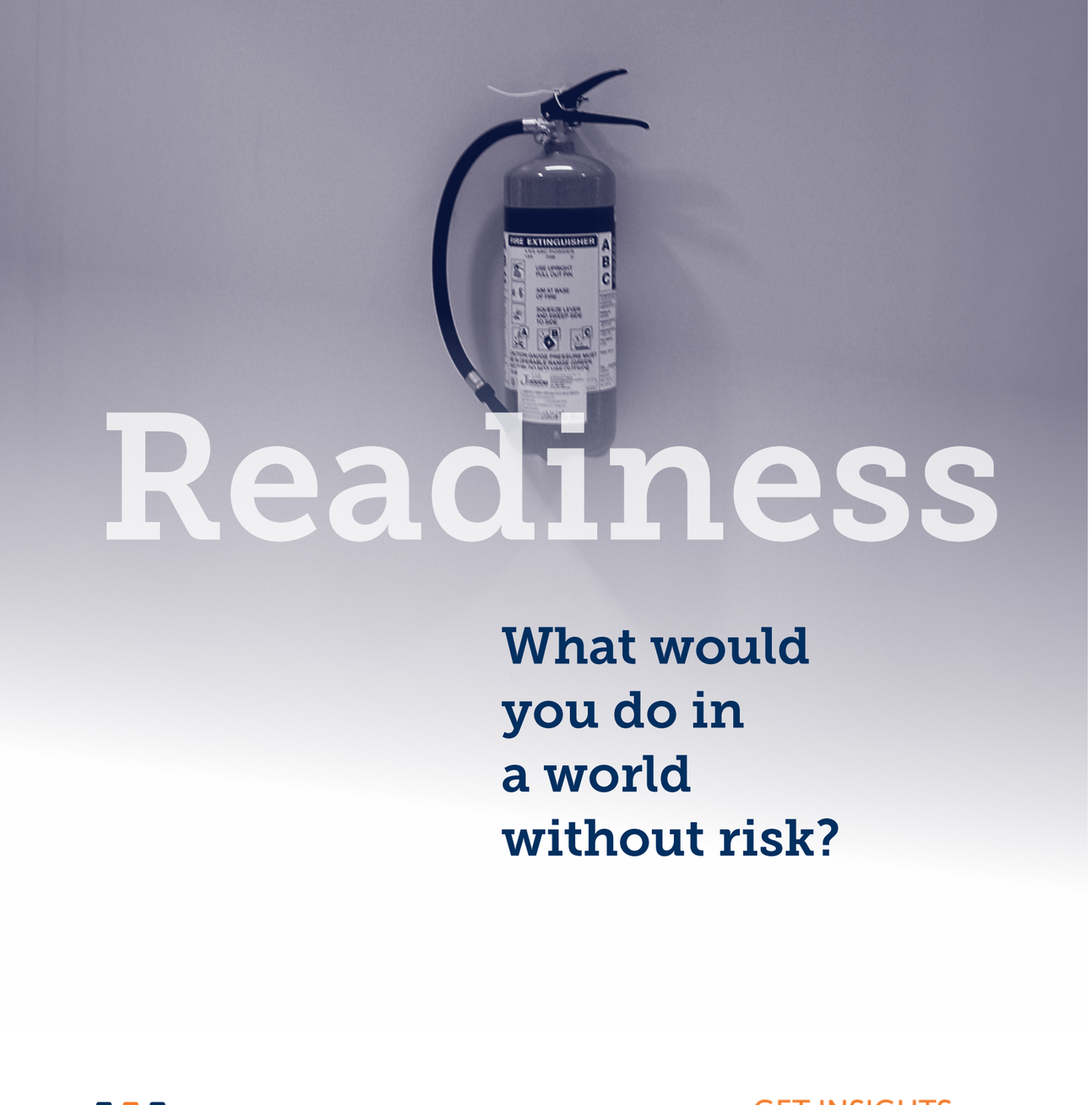
RC ANSWERS:
Should small to medium-sized businesses care about cyber risk?

Meet Our Featured Risk Leader: Yvette Connor

Disaster recovery: costliest year on record?

" Risk is either a cost or a catalyst, you choose."

Risk Cooperative



Readiness

What would you do in a world without risk?

Contents

"Risk can be measured, uncertainty cannot. Risk creates profits and losses, uncertainty creates bank runs."

COLUMNS

FEATURES

Risk Matters

Risk Cooperative
1140 Connecticut Ave., NW
Suite 510
Washington, D.C. 20036

+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

2017 has proven to be an *annus horribilis* for complex risks. Whether you are measuring the seemingly endless volley of technological and cyber threats, which with the Equifax breach alone impacted more than 143 million people, or the troubling normalcy of political risk, the case for resilience never seemed more urgent.

The real antagonist this year was not an opaque cyber ne'er-do-well or an errant politician sowing havoc, but rather 2017 was the year climate risks took center stage. This year's hurricane season for example saw no less than 3 record-breaking storms, beginning with Hurricane Harvey's "nuclear rain bomb," which dropped more rain on the city of Houston than had ever been recorded in the U.S. Hurricane Irma, at once the most powerful and persistent Atlantic hurricane, delivered a one-two punch to the Caribbean with her sister storm, Hurricane Maria, which destroyed Puerto Rico and the U.S. Virgin Island's enfeebled infrastructure. Puerto Rico now has the dubious distinction of playing host to the longest running blackout in U.S. history, crossing the 70th day with the prospects of many months more before power is fully restored. Apocalyptic wildfires in California, coupled with devastating seismic and volcanic activity around the world will conspire to make 2017 the costliest year for climate-related disasters.

While the human and economic costs of these and other disasters are still being tallied, it is very likely 2017 will be a $500 billion year in terms of financial losses. Against this backdrop of so much misery and property loss, two opportunities emerge. The first is to take the business case of pre-investing in resilience, particularly when it comes to climate change, seriously. The second is to take the opportunity presented in foundational technologies like Blockchain as part of our toolkit to drive down rates of institutional mistrust, underinsurance and currently uninsurable risks, which end up being funded by taxpayers.

If there is one enduring lesson from 2017, it is that we are firmly in an invest now or pay latter world, but either way we are going to pay. This issue of Risk Matters looks at risk, readiness and resilience through this lens.

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

Featured Risk Leader

Yvette Connor is the Chief Risk Officer (CRO) of Focal Point Data Risk, LLC and head of the firm's Enterprise Risk Consulting practice. With more than 20 years of experience building, implementing, and testing enterprise risk frameworks, she specializes in building effective enterprise risk management (ERM) programs for Focal Point's clients using decision-driven models informed by enterprise risk factors and organizational behavior. Ms. Connor also oversees the firm's work behind the acclaimed Cyber Balance Sheet Report, a first-of-its-kind research study that looks at the cyber risk issues resonating in boardrooms.

YVETTE CONNOR, CHIEF RISK OFFICER AT FOCAL POINT DATA RISK

Before joining Focal Point in 2017, Ms. Connor was a Managing Director at Alvarez & Marsal Insurance and Risk Advisory Services, where she focused on global ERM engagements and developed a unique approach for enterprise-wide cyber risk valuation.

While serving at Marsh, Inc. as the Director of Client Engagement, she managed Marsh 3D, a global servicing model designed to define clients' needs and risk priorities and create optimal risk management responses and value-add solutions. In addition, she was the lead designer for Marsh's Dynamic Risk Mapping tool.

Prior to joining Marsh in 2010, Ms. Connor was the Director of Risk Management at Vulcan Inc., where she led the development of a multi-disciplinary risk management department and rolled out an enterprise-wide risk management framework across a portfolio of stakeholders and companies.

Beyond these roles, Ms. Connor is also a thought leader on emerging risks and strategies for effectively managing risk and integrating ERM frameworks with cyber security, compliance, and audit platforms. Her research has focused both on the ways companies identify risk priorities broadly throughout an organization and more narrowly, by delving deeper into specific risk areas. Ms. Connor earned both a master of science in risk management and a MBA in finance. Her master's thesis "Does Risk Management Matter to Shareholders" describes a methodology to financially assess the impact of "sophisticated" risk management on both profitability and growth.

In 2013, *Business Insurance* magazine named Ms. Connor as one of the "Women to Watch" in Risk Management and Insurance, and in 2008, *Treasury and Risk* magazine recognized her as a rising leader in treasury risk, as part of their "40 under 40" list.

With an impressive track record of forward-thinking, client-focused ERM strategies and tools, *Risk Matters* names Yvette Connor our Risk Matters Featured Risk Leader.

RISK MATTERS | FALL 2017

By the Numbers

2017 IS AMONG THE COSTLIEST CATASTROPHE LOSS YEARS IN U.S. HISTORY[1]

Cost to **insurers** due to national catastrophes[2] **$100 BILLION**

Premiums may see increases[1] **UP TO %50**

HURRICANES
Harvey, Irma and Maria wrought catastrophic damages

$45 – 95 BILLION
Cost to **Puerto Rico** from Hurricane Maria[3]

$3 BILLION
Cost to **AIG** from Hurricanes Maria, Harvey & Irma[4]

$180 BILLION
Estimated cost of Hurricane Harvey[5]

FLOODING
Houston suffered record breaking floods

LESS THAN 20%
Insured via flood insurance program for Hurricane Harvey[6]

UP TO 85%
Homeowners in Houston have no flood insurance[7]

WILDFIRES
Over 20 fires burned in Northern California

$5 – 8 BILLION
Cost of California wildfires[9]

[1] http://www.propertycasualty360.com/2017/11/21/2017-to-be-one-of-the-costliest-catastrophe-loss-y
[2] http://www.businessinsider.com/hiscox-insurance-natural-disasters-100-billion-2017-11
[3] http://www.businessinsurance.com/article/00010101/STORY/912316192/Hurricane-Maria-likely-to-cost-Puerto-Rico-up-to-$95-billion-Moodys
[4] http://fortune.com/2017/10/10/aig-hurricane-season-damage-cost-impact/
[5] http://fortune.com/2017/09/03/hurricane-harvey-damages-cost/
[6] https://www.usatoday.com/story/money/2017/08/29/insurance-woes-await-flood-victims-under-covered-houston-area/613239001/
[7] https://qz.com/1063985/hurricane-harvey-why-85-of-homeowners-in-houston-dont-have-federal-flood-insurance/
[8] https://www.insurancejournal.com/news/international/2017/09/29/465995.htm
[9] http://www.insurancebusinessmag.com/us/news/catastrophe/forget-3-billion--california-wildfires-could-cause-much-higher-insured-losses-says-aon-83252.aspx

Summaries

BLOCKCHAIN COULD MAKE THE INSURANCE INDUSTRY MUCH MORE TRANSPARENT | PUBLISHED 07.12.2017

Written by Dante Disparte
Originally published on HBR.org

Blockchain is set to transform the insurance industry through the distributed ledger, which exposes aspects of the insurance value chain that have been based on utmost good faith for ages. While painful for some industry players, Dante Disparte argues that this transparency is badly needed to overcome a lack of trust in the the financial sector and boost penetration in underinsured markets.

Read the full article: https://hbr.org/2017/07/blockchain-could-make-the-insurance-industry-much-more-transparent

IF YOU THINK FIGHTING CLIMATE CHANGE WILL BE EXPENSIVE, CALCULATE THE COST OF LETTING IT HAPPEN | PUBLISHED 06.12.2017

Written by Dante Disparte
Originally published on HBR.org

Dante Disparte offers a counter-argument to the rationale for pulling out of COP21—that climate change itself it terribly expensive and inseparable from economic and other risks, and that investing in climate resilience offers incredible economic opportunities.

Read the full article: https://hbr.org/2017/06/if-you-think-fighting-climate-change-will-be-expensive-calculate-the-cost-of-letting-it-happen

GDPR AND THE INFORMATION SECURITY ARBITRAGE | PUBLISHED 8.24.2017

Written by Dante Disparte and Chris Furlow
Originally published on International Policy Digest

General Data Protection Regulation (GDPR), as our recent Risk Matters video outlines, is a global issue that keeps risk leaders up at night. Chris Furlow and Dante Disparte collaborate to explain several possible ways (beyond fundamental compliance) that GDPR enforcement may impact business as usual.

Read the full article: https://intpolicydigest.org/2017/08/24/gdpr-information-security-arbitrage/

THE I OF VERY BIG T: (IOT RISKS) | PUBLISHED 08.21.2017

Written by Dante Disparte
Originally published on Huffington Post

When we consider the Internet of Things (IOT) we often think of home appliances and the risks of exposing our personal data. But Dante Disparte reminds us that much larger things are also online, including aircraft and electrical grids. How vulnerable are these very big "things?"

Read the full article: https://www.huffingtonpost.com/entry/the-i-of-very-big-t-iot-risks_us_5998b70fe4b03b5e472cf042

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

Featured Analysis

BLOCKCHAIN AND THE POWER OF SINGULARITY | PUBLISHED 08.1.2017

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 poorly named crypto currency market. BitPesa has received UK regulatory

RISK MATTERS | FALL 2017

Featured Analysis

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 cyberthreats 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://www.huffingtonpost.com/entry/59806b85e4b07c5ef3dc1808

THE BEST CYBERSECURITY INVESTMENT YOU CAN MAKE IS BETTER TRAINING | PUBLISHED 05.16.2017

Written by Dante Disparte and Chris Furlow
Originally published on HBR.org

As the scale and complexity of the cyber threat landscape is revealed, so too is the general lack of cybersecurity readiness in organizations, even those that spend hundreds of millions of dollars on state-of-the-art technology. Investors who have flooded the cybersecurity market in search for the next software "unicorn" have yet to realize that when it comes to a risk as complex as this one, there is no panacea — certainly not one that depends on technology alone.

Spending millions on security technology can certainly make an executive feel safe. But the major sources of cyber threats aren't technological. They're found in the human brain, in the form of curiosity, ignorance, apathy, and hubris. These human forms of malware can be present in any organization and are every bit as dangerous as threats delivered through malicious code.

With any cyber threat, the first and last line of defense is prepared leaders and employees, whether they are inside an organization or part of an interconnected supply chain.

And yet organizational leadership all too often demonstrates outright technology torpitude. An unprepared, lethargic leadership only amplifies the consequences of a security breach. The scale of the Yahoo breach disclosed in 2016, combined with the fumbling response, cost the company and its shareholders $350 million in its merger with Verizon and nearly scuttled the entire deal.

Featured Analysis

To prepare for and prevent the cyberattacks of the future, firms need to balance technological deterrents and tripwires with agile, human-centered defenses. These vigorous, people-centric efforts must go beyond the oft-discussed "tone at the top" — it must include a proactive leadership approach with faster, sharper decision making. As cyber threats grow exponentially, comprehensive risk management is now a board-level priority. Indeed, the iconic investor Warren Buffett highlighted cyber risk as one of the gravest concerns facing humanity during Berkshire Hathaway's annual meeting.

Firms must recognize and react to three uncomfortable truths. First, cyber risk evolves according to Moore's Law. That's a major reason that technology solutions alone can never keep pace with dynamic cyber threats. Second, as with all threat management, defense is a much harder role to play than offense. The offensive players only need to win once to wreak incalculable havoc on an enterprise. Third, and worst yet, attackers have patience and latency on their side. Firms can be lulled into a dangerous state of complacency by their defensive technologies, firewalls, and assurances of perfect cyber hygiene.

The danger is in thinking that these risks can be perfectly "managed" through some sort of comprehensive defense system. It's better to assume your defenses will be breached and to train your people in what to do when that happens. Instead of "risk management," we propose thinking of it as "risk agility." The agile enterprise equips all organizational layers with decision guideposts and boundaries to set thresholds of risk tolerance. All employees should not only understand what is expected of them regarding company policy and online behavior but also be trained to recognize nefarious or suspicious activity. The key attribute, particularly when it relates to cyber risk, is the concept of sense something, do something, which makes all people in an organization a part of a "neural safety network." For example, the defense against the SWIFT banking hack, which saw some $81 million be stolen, was launched by an alert banking clerk in Germany who recognized a misspelling.

When we say all employees have to be risk agile, we mean all. C-level executives, board directors, shareholders, and other senior leaders must not only invest in training for their firm's own employees but also consider how to evaluate and inform the outsiders upon whom their businesses rely — contractors, consultants, and vendors in their supply chains. Such third parties with access to company networks have enabled high-profile breaches, including Target and Home Depot, among others.

A skeptical executive could push back on this idea — won't that cost a lot? The fact is, cybersecurity training is vastly undercapitalized, and the lack of investment in quality cyber education programs is manifest in the sheer volume of breaches that continue to be rooted in human failure. Worse, the volume of breaches is woefully underreported — even when they are identified early because firms are reluctant to amplify reputation risk. In a 2016 survey conducted by CSO magazine and the CERT Division of the Software Engineering Institute of Carnegie Mellon University, respondents reported that insiders were the source of "50% of incidents where private or sensitive information was unintentionally exposed." Insider threats can include malicious activities but also mistakes by employees, such as falling for a phishing scam.

In short, there will be some investment required in enhancing personnel readiness. But it can be cost effective over time, particularly when compared to implementing cutting-edge cybersecurity technology that may become obsolete. To be clear, technology is a critical piece of the cybersecurity puzzle, but just as with a car containing all the latest safety technology, the best defense remains a well-trained driver.

Moreover, businesses slow to adopt stronger security measures may find themselves pushed into it by regulators. The latest regulations promulgated by the New York State Department of Financial Services, for example, requires that covered businesses "provide regular cybersecurity awareness training for all personnel." This is just the tip of the iceberg of what is likely to come from other states and government agencies around the world, which are increasingly harmonizing their view of a "carrots and sticks" approach to cybersecurity compliance.

Artificial intelligence, machine learning, and self-teaching algorithms may represent the latest trends in hot IT investments, but technology exists for and is utilized by people. Corporate leaders would be wise to understand that the future of cybersecurity lies not in a single-pronged approach or miracle tool but in solutions that recognize the importance of layering human readiness on top of technological defenses.

https://hbr.org/2017/05/the-best-cybersecurity-investment-you-can-make-is-better-training

BRUNSWICK INTERVIEW: UNDERWRITING THE UNMEASURABLE | PUBLISHED 07.13.2017

Written by Siobhan Gorman
Originally published on Brunswick Review

Risk Cooperative CEO Dante Disparte sits down with Brunswick's Siobhan Gorman to discuss how cyber attacks are redefining what "risk" means for M&A

The infamous political adviser Niccolò Machiavelli wrote, "Never was anything great achieved without danger." Sage words for an aspiring politician, but not comforting for CEOs leading what they hope are transformative mergers or acquisitions.

Executives overseeing deals have undoubtedly heard that their businesses are vulnerable to cyber attacks. But how much more vulnerable are they when hosts of advisers and third parties are involved, millions – or billions – of dollars are at stake, and employees, customers, regulators, investors, and even the media are watching closely? The fallout from a 2016 cyber attack on Yahoo!, as it was in the process of being acquired by Verizon, lowered the deal's price tag by $350 million.

In response to this growing threat, and amid an uptick in global M&A activity – which climbed almost 9 percent in Q1 2017 (see "Dealmakers see 'Trump Bump,'" Page 10, for more insight) – a niche solution to manage cyber risk is gaining popularity: insurance policies tailored to cover the damage caused by cyber attacks during M&A.

Dante Disparte is CEO of Risk Cooperative, which operates at the intersection of three complicated, technical fields: insurance, risk management and cybersecurity. In a conversation at Brunswick's Washington, DC office, from which this interview is

RISK MATTERS | FALL 2017

Featured Analysis

excerpted, Disparte acknowledged the challenge of quantifying the risk a cyber attack poses. "The events that are much harder to measure are the ones that scare us: the theft of IP, crippling of systems, permanently rendering data useless."

Today, having cybersecurity policies during an M&A, or even conducting basic cyber due diligence, aren't regulatory requirements. Disparte thinks that's likely to change. But rather than simply a compliance box to tick, Disparte believes the best practices and transparency involved in insurance have a much broader role to play, acting as "a catalyst for business rather than a cost of business."

What cyber threats are unique to M&A?
One big one – we actually call this kind of concept, "cyber-cultural assimilation." To use a metaphor: in a car with all the safety technology in the world, the best defense is a well-trained driver. We think that the human factor in cyber risk is an enormous gap.

And clearly in an M&A scenario, you run a very high risk of alienating staff in the acquired company. People might think through what role they have in the post-merger world, if any. That's an enormous area of opportunity for improvement: in any M&A transaction, how do you get the human element brought into light and focus?

How can businesses manage the flood of cyber risks that accompany a merger?

I think step one is to never assume that the current due diligence frameworks pick up cyber risk.

Why?
When companies go into an M&A scenario, oftentimes for regulatory reasons or competitive reasons, it goes into a very silent, hermetically-sealed black box. And the tools that we currently have in our arsenal today – legal background, financial due diligence – often only the board or the C-suite will know about these possible talks. Any leak will have potential damage. So, the toolset really is not picking up cyber exposure. We need a slightly more invasive process, which will create some discomfort and transparency, but will ultimately enable M&A.

How do you create more transparency, and how do you get both companies on board?
I think you need to have a model in which the acquired company and the acquirer are coming into this under the view that, absent a deeper level of due diligence around cyber risk, the deal may not go through – almost a good-faith mechanism.

Can insurance help solve such a big problem?
In the insurance and technological industry around cyber risk mitigation, we most often get called almost like the fire brigade – when there's a problem. Many of the tools that we rely on, whether it's endpoint threat detection systems or crisis management, are of the "break in case of emergency" variety.

But imagine if you brought that capability into the deal room, if you will. Now instead of waiting for a crisis to emerge before you're addressing it, you're embedding that capability as a part of the investment review process. Suddenly, you now have a mitigation strategy around different scenarios. It's an issue, in my mind, of enabling these deals to go through in the first place at fair market value – as opposed to stopping them altogether or, worse yet, having the market decide how to price these risks.

Insurance in cyber is harder to gauge than, say, health insurance, where you have a track record and a lot of data you can point to.
In my view, cyber is more akin to life insurance; if you're buying a high-value life insurance policy, the underwriter doesn't just take your word for it. They actually go check your blood.

I think it's critically important for insurers, people like myself and companies like ours to not just take the customer's word for it, but to do endpoint-level threat detection to understand the hygiene of an enterprise and how it evolves over time.

Then we underwrite cyber risk using an evidenced-based approach. Two houses are insurable, but the one with smoke detectors, sprinklers and an alarm system is a better risk. We apply a system of credits and debits to cyber risk as we're working through underwriting them. We see cyber as a standalone risk. It needs a standalone solution – that only makes up 5 percent of the market today. The rest is what I call a "Frankenstein policy," it's bundled alongside other classes of insurance.

Cyber risk is woefully underfunded and unhedged – to the tune of trillions of dollars of market value. A lot of firms are going to find themselves either in courtrooms or getting short shrift when it comes to this exposure and a similar number of investors may find themselves facing unforeseen losses.

What is the biggest misconception you see with cyber insurance? What are people not getting?
Well, one, they're not getting it enough. Because in part there's the placebo effect. Many believe that this risk may be covered elsewhere in their insurance and risk management framework.

A lot of it is also internal; if you're the chief information security officer of even the very biggest companies on the planet, you have a powerful inducement to say "It's all fine." It's called paycheck persuasion, hubris, organizational silos and territorial defense.

Cyber does not singularly reside in IT. It's a governance issue, it's an enterprise issue. And it starts at the C-suite and board levels. They're the ones who own the risk at the end of the day, not the IT security professionals, not the marketing and public relations professionals. There we find that there's a lot of work to be done yet. If you need help with your iPad, you are going to have a hard time in a boardroom asking questions and querying the state of play inside an organization's risk management frameworks.

What do you say to leaders who say: "I get that cybersecurity is an issue, but I'm going to invest in better, secure systems, not insurance?"
I would say, "Great, prevention is often better than cure. But I think a part of the whole spectrum of solutions needs to incorporate equilibrium." All too often you have enormous financial institutions spending hundreds of millions of dollars on cybersecurity, and it is easy to gravitate toward spending money on technology.

But this is a risk for which there isn't singularly a technological solution. Cyber risk advances according to Moore's law; bad actors have the benefit of patience and the organization and staff are the first lines of defense.

https://www.brunswickgroup.com/underwriting-the-unmeasurable-i5215/

RISK MATTERS | FALL 2017

Featured Analysis

THE EQUIFAX BREACH AND 5 YEARS OF MISSED WARNING SIGNS | PUBLISHED 09.18.2017

Written by Dante Disparte
Originally published on Huffington Post

Reports that Equifax's chief information officer along with their chief security officer were retiring should alleviate few concerns and not divert scrutiny from the company's risk governance standards. While this is not the largest data breach in history, it is quite possibly the most damaging. This data breach is different in kind and much more harmful than anything before it, primarily because it reveals personally identifiable information on nearly 100% of the U.S. workforce, as well as private information on consumers from other countries. Had Europe's General Data Protection Regulation (GDPR) been in force, Equifax would not only face the raft of litigation in the U.S., alongside a growing number of government investigations, it would also be in breach of the world's most stringent privacy standards – resulting in hefty fines of up to 4% of the company's worldwide sales or €20 million. While the company's technology leaders were quick to fall on their own swords, this case reveals that cyber security is an executive level priority inconveniently cutting across the c-suite and not a risk that conforms to clean organizational siloes. The Equifax breach is another painful example teaching us that cyber resilience begins and ends with the board and senior executives. What Equifax's annual reports tell us about their attentiveness to risk, readiness and resilience is alarming.

While Equifax is undergoing a mounting barrage of regulatory, legal, consumer and investor scrutiny, including from the Federal Trade Commission, the firm's demonstrated risk awareness in its annual reports leaves little room for doubt. It would appear that at Equifax, customers (banks and lenders that want to gauge people's credit worthiness), growth, shareholders and investors mattered more than managing cyber risk, privacy or information security. In a keyword search through 5 years' worth of Equifax annual reports, terms that would suggest adequate risk awareness, such as risk management, cyber risk, privacy, data security, data breach or information security, barely appear at all. In fact, the term cyber risk does not appear once in any of the credit bureaus' annual reports in the last 5 years. This certainly should give all market participants pause as companies that quite literally hold the "crown jewels" on hundreds of millions of people are nothing more than data and information technology firms for which cyber threats can be existential. But how does Equifax stand up to its peers by this measure?

Against the same measure, in looking at the annual reports of the 3 major credit bureaus for a 5-year period conducting the same keyword searches reveals a general lack of risk awareness when it comes to information security and privacy. Of the 3 firms in question, arguably Experian is the best of the worst alternatives, in part because of its headquarters in Ireland, wherein the EU has more stringent privacy and cyber security standards. Of the 2 major U.S. credit bureaus, TransUnion and Equifax, TransUnion would score higher through this somewhat crude measure of risk awareness and risk governance. Up until now the business models of major credit bureaus relied in part on a moral hazard, which is risk taking without bearing the consequences. This is so because these are largely business-to-business firms and they typically do not trade with retail customers, whose data they store and analyze. The Equifax breach and its massive fallout will likely resolve this moral hazard as regulators are sure to change laws on consumer privacy and protection following this case.

It should be no surprise then that Equifax comes at the bottom of this benchmarking analysis, where keywords demonstrate a general lack of awareness and appreciation for how cyber threats prey on firms of this nature. It is also telling to watch the evolutionary property of risk awareness over the 5-year period across all 3 firms. What is clear across the spectrum, and this is certainly not uncommon for large enterprises, is that growth, shareholders, investors and profitability are key priorities that often trump adequate risk management, which is all too often consigned to a loss prevention or decision avoidance function. In short, risk management is treated like a cost center. This much rings true in this cursory analysis of the 3 major credit bureaus. Adjusting for a more than 30% decline in Equifax's share price, or $6 billion in market value, however, the often intangible value derived from risk management is made clear. Similarly the need for a universally accepted measure of the enterprise value of data is made all the more urgent due to this breach.

Confronting risks head on and certainly disclosing them in annual reports should not be a regulatory requirement, but rather something executives provide in the spirit of transparency, trust building, and as a source of competitive advantage. Risks are complex, but over the 5-year period of this analysis one would be hard-pressed to find a senior executive who was not concerned with the growing rise and interdependency of technology and with it cyber threats. Over the same timeframe there have been many major breaches, which if nothing else should signal to information technology companies that these risks should be taken seriously.

Facing massive legal battles and regulatory scrutiny, which will soon see Equifax's CEO called before Congress for the usual indignation that follows these large scale corporate lapses, key questions need to be asked of how the world can mitigate such a systemic threat. The first and last line of defense against complex risks is to have strong corporate value systems and governance standards. Aside from the fact that many systemic firms are hiding in plain sight, perhaps the most enduring management lesson from the Equifax breach is that board members and executives should not wait for regulatory pressure before they begin disclosing a true risk-adjusted picture of their enterprises. For companies that own cyber risk in this manner they can gain risk agility instead of being caught flat-footed by so-called surprise events.

https://www.huffingtonpost.com/entry/the-equifax-breach-and-5-years-of-missed-warning-signs_us_59bf2480e4b06b71800c3b07?utm_source=RC+Insights&utm_campaign=245551c598-August_Insights_8_2_2017&utm_medium=email&utm_term=0_c44bac8238-245551c598-

RISK MATTERS | FALL 2017

Featured Analysis

CLIMATE RESILIENCE: NO LONGER ISLANDS UNTO OURSELVES | PUBLISHED 09.21.2017

Written by Dante Disparte
Originally published on Huffington post

No sooner than the record-breaking hurricane Irma wrought havoc across the Caribbean as the most powerful and persistent Atlantic storm ever, the region braces for yet another monster category 5 hurricane with Maria. Maria, the first major hurricane to make direct landfall on the U.S. territory of Puerto Rico in more than 85 years, has devastated the island. Islands are particularly vulnerable to climate risks and are fast becoming ground zero in our rapidly changing world, reminding us that in the face of unprecedented challenges, we can no longer be islands unto ourselves.

An emblem of this devastation is the fact that the inhabitants of the once idyllic island of Barbuda, along with other islands in the region, are now veritable climate change refugees. For the first time in more than 300 years, Barbuda is totally uninhabited by people. These same displaced people, along with residents of other Caribbean islands, are finding little solace as one of their places of refuge in Puerto Rico, which was spared the worst of hurricane Irma, is now ground zero for hurricane Maria. Amid the regional ruin, rich and poor alike were not spared the devastation, proving that nature's arsenal is just as indiscriminate as ours.

Indeed, Sir Richard Branson, who weathered hurricane Irma in his wine cellar on Necker Island, has marshalled his considerable brand presence to raise awareness, resources and global support for a region he calls home. Even with formidable voices like Branson's sounding the alarm, the world's media cycle and disaster response resources are barely keeping pace with hurricane Harvey and its nuclear rain bomb, which devastated Houston, Irma's aftermath in the Caribbean and across the entire Florida peninsula, and most recently, a horrific earthquake in Mexico, which has claimed more than 200 lives. All the while, the drum beat of war grows ever louder with President Trump's ominous speech at the UN General Assembly, in which he offered to wipe North Korea off the map. Perhaps in a time of great national peril and global need, the U.S. should be less concerned with destroying nations and more concerned with shoring them up.

Puerto Rico's already dilapidated power grid, which failed in 2015 plunging the island into darkness due to underinvestment, will likely take months to restore following island-wide power outages. Indeed, Irma and Maria delivered a particularly vicious one-two punch to the region. Where on the one hand Irma spared Puerto Rico, still leaving more than 1 million residents without power and 60,000 without water, Maria completed the job delivering a knockout blow.

The sum of these terrible events – remembering that hurricane season is not over yet and these tropical storms are not the only threat islands face – begs the question, what can be done to reinforce pan-Caribbean resilience and disaster preparedness? The first step, which heartening scenes of solidarity across the region remind us of, is to remember the connections that bind the islands to one another and to the rest of the world. These grim scenes are very much what climate change looks like and the prospect of national-level resettlement is already upon us, albeit on a much smaller scale.

While property and material effects can be replaced, lives and livelihoods cannot. For a region that largely depends on tourism for its GDP, the world has a special obligation to revisit the Caribbean just as soon as the winds and tides subside. In the meantime, the long road to recovery begins and some unique opportunities to improve regional resilience emerge. Chief among these is the need to deepen insurance penetration across the region, improving the scope of coverage to reflect the growing severity of climate risks. Lloyd's research shows that a 1% increase in insurance penetration translates into a 22% reduction in the tax-payer burden of unfunded financial losses. Another challenge plaguing insurance across the Caribbean basin is that natural catastrophe models used by insurers to determine premium rates lump the Caribbean and the Florida peninsula into one super-region. While both areas are clearly disaster prone, property replacement costs, building codes and labor rates, to name a few categories, are not the same. Calibrating insurance and reinsurance rates not just in the Caribbean, but globally, adjusting for purchasing power can go a long way in improving market adoption and affordability.

Similarly, the creation of a pan-Caribbean risk-sharing pool that can proportionally aggregate financial resources for natural disasters can help shore up the wider region and, in particular, the most vulnerable islands. Paying into this regional reinsurance program can also enable the acquisition and maintenance of the response materiel needed for a wide variety of events, such as a flotilla of response vessels, generators, non-perishable food items, temporary shelters, among others. Another critical area of improvement is the region's energy matrix. All too often Caribbean economies rely on dated, inefficient and polluting energy sources to power the grid. If there is any region in the world that speaks to the case for energy diversification, the Caribbean is it.

The collapse of Venezuela's oil for influence program, Petrocaribe, set the stage for alternatives to take root. Having said that, the U.S. perilously clings to the Jones or Merchant Marine act, which senselessly compounds the price of goods – including fuel oils – shipped to Puerto Rico, while cutting the number of vessels that can sail to the island by more than half. Puerto Rico's comparative resilience to its neighbors and the fact that it is the southernmost U.S. territory and a natural logistics hub – once home to large U.S. military installations – makes it the perfect staging ground to not only coordinate acute response efforts, but to lead long term regional initiatives that improve Caribbean resilience.

As with all cases of climate threats, whether in the Florida Keys, Houston or in San Juan, human habitation is failing to keep pace with the rate of change. Building codes must be updated to reflect more extreme – "out of sample" – weather events. Similarly, we must urgently address the lack of affordable and resilient housing across the region, as well the lack of shelters for vulnerable communities. The pain and destruction left in the wake of hurricanes Irma and Maria are stark reminders that in the face of climate change we can no longer go it alone.

https://www.huffingtonpost.com/entry/59c2c661e4b0ffc2dedb5aa9

RISK MATTERS | FALL 2017

Featured Analysis

FROM TECH TITANS TO BLOCKCHAIN BILLIONAIRES | PUBLISHED 08.30.2017

Written by Dante Disparte
Originally published on Forbes.com

If the internet augured a world of frictionless information sharing, can blockchain augur a world of frictionless value transfer? A standards war – or better still a use case knife fight – is being waged among blockchain technology companies large and small, as well as a raft of consultants who are pitching every novel blockchain use case to anyone who will listen. The industry and world-changing outcomes that are promised are few and far between in the real world, with the exception of blockchain's so-called "killer app," Bitcoin and its digital currency brethren. And yet, however fleeting or threatening the prospect of a low-friction economy may seem to established players, blockchain is here to stay and its power to transform, augment and disrupt may very well surpass the internet's.

A growing cadre of people are recognizing that blockchain is in fact the "killer app" of the digital currency era, going as far as likening it to a foundational technology. A growing number of entrepreneurs and investors are crowding in to the blockchain space all seeking to answer the core question: "If blockchain could not exist without the internet, what could not exist without blockchain?"

It is this wave of creation, much like the early days in any emerging industry, that will drive the most profound change in the global economy minting a new generation of Tech Titans – call them Blockchain Billionaires. In 1994, when Amazon was founded setting a young Jeff Bezos on a path toward an $83 billion personal fortune, it was easy for retailing stalwarts like the 124-year-old Sears, which is wrestling with financial risks, along with the equally troubled J.C. Penney to dismiss the concept of online commerce or assume that "try before you buy" consumer behavior was a steady state. It turns out that neither assumption was constant with some existential consequences for traditional retailers that ignored opportunity's knock.

Much like Blockbuster met its demise by not opening the door to the internet and the concept of content streaming, established businesses and institutions may meet a similar fate for ignoring blockchain's call to action. The most enduring firms that roared through the internet bubble and the new breed of sharing economy giants, like Uber and Airbnb, have created outsized value by providing people with what they want in the real world.

At our core, people want less friction in their lives, they want more trust in their relationships, personal, professional and institutional, and perhaps most profoundly, they want common witness to their claims of value. For this reason, some of the larger blockchain implementations outside of the digital currency market have focused on reducing the friction while increasing the trust and security of land titling.

For most people – at least those that have the fortune of ascending Maslow's slippery economic pyramid – land and property represent their single largest assets. And yet, the drag coefficient, friction and opacity surrounding the lifecycle of this asset class labors under the weight of costly and inefficient intermediation, and, worst yet, risk-prone paycheck persuasion. The result is that affordable homeownership is aspirational for most. For the lucky ones who cross this threshold they are often burdened with "trust-inducing" private mortgage insurance (PMI) as a condition of their loan, all to acquire an asset that can be whisked away from them with a stroke of a pen.

In advanced economies, this event tends to be rare under the banner of eminent domain. However, in many developing and emerging countries land rights often shift with impunity behind the firewall of centralized record keeping. The only public defense against this impunity is the collective memory and power of common witness. Blockchain-based land registries are the 21st century equivalent of an entire village bearing witness to an unalterable transaction.

The advent of blockchain technology is not a zero-sum proposition for established industries and institutions, although it can be profoundly disruptive for late adopters. Instead, blockchains can become an enduring part of a business model or operating process provided they connect to the things people value. While much analysis on blockchain tends to focus on the business impacts in finance and supply chain management, the opportunities, especially in the e-governance arena are bigger. Imagine modernizing campaign finance, for example, with a verifiable single-citizen token that tracked a political contribution from origination to candidate.

Not only would this make the process much more efficient, it may very well accelerate and, critically, flatten the revenue model such that all viable candidates operate on common ground. Without blockchain, this type of idea would be dead on arrival, for all current alternatives grind with the friction of centralization and special interests. The era of Blockchain Billionaires and digital transformation is upon us and those that succeed will connect to enduring values and interests the way the Tech Titans have before them

https://www.forbes.com/sites/dantedisparte/2017/08/30/from-tech-titans-to-blockchain-billionaires/#11fb29472428

RC Answers

Should small to medium-sized businesses care about cyber risk? Should they insure against these threats?

The short answer is yes. Unlike large organizations, which often have a "fortress balance sheet" that can absorb financial losses or business interruption, small to medium-sized enterprises (SMEs) are not afforded the same luxury. Additionally, during a cyber-attack, breach or ransomware, the so-called fire brigade we all call upon are skilled cybersecurity technicians. In these cases, many larger enterprises (although the headlines are proving their vulnerability), can call on their internal cybersecurity teams. Here too, SMEs often have a light cybersecurity or IT bench, making them easy pretty for cyber risks.

Another common misperception among SMEs is that they carry little or no sensitive information (what is commonly known as personally identifiable information, PII, in cybersecurity parlance), therefore they have little risk or compliance obligations. This could be further from the truth, as the types of cyber threats increasingly have less to do with data breaches and more to do with holding organizations "hostage" by crippling their systems. The Target breach of 2013, for example, was carried by exploiting vulnerabilities in one of their heating and cooling vendors, which created a "backdoor" into Target's systems. As many SMEs are often in the supply chains of larger firms or are themselves government contractors, carrying cyber insurance is increasingly mandated. In a word, cyber risk is a systemic threat and all organizations, large or small, should treat it as a stand-alone enterprise risk requiring stand-alone risk management and insurance.

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 BECOMES LLOYD'S COVERHOLDER, 3RD ANNIVERSARY

Coverholder at LLOYD'S

On the verge of Risk Cooperative's third anniversary, the firm has become a coverholder at Lloyd's, for our unique cyber insurance capability. 3-year-old Risk Cooperative and 330- year-old Lloyd's, unite in a unique business model whereby Lloyd's, the world's specialist insurance market, relies on firms like Risk Cooperative for market access, innovation and distribution.

360° CYBERSECURITY REPORT

DOWNLOAD

Designed to evaluate the state of cyber readiness amongst respondents, largely comprised of middle market firms across a range of industries, the report sheds light on the key challenges firms are facing across the cyber threat landscape. The 360° Cybersecurity Report highlights industry agnostic trends, best practices, and insights to emerging cyber vulnerabilities.

Cybersecurity remains a top of mind concern for executives struggling to grapple with this fast-evolving risk. This report will help organizations understand the financial and reputational impacts posed by cybersecurity risks as well as what solutions can help firms remain resilient across all industries and sizes.

While many larger enterprises can "throw money at the issue", cybersecurity risk represents an existential threat for many others—particularly middle-market organizations. Aronson's partners are committed to helping our clients address these types of risks and emerging challenges. Our partnership with Risk Cooperative, and Ridge Global, as well as the insights gleamed from this report, will help the development of customized solutions to help our clients better prepare and defend their organizations against cyber risk.

STRATEGIC PARTNERSHIPS

The Risk Cooperative has announced a number of innovative partnerships in recent months.

Among the most exciting developments, is a noteworthy strategic partnership with Bitfury to use blockchain in the insurance broker market. This news was reported on by the New York Times, Reuters, and Insurance Journal in June.

Also in June, AchieveNext and the CFO Alliance announced that it will work with Risk Cooperative to expand it's portfolio of solutions designed to support corporate excellence.

A month earlier, Emerge Education announced a ipartnership with Risk Cooperative to offer risk transfer solutions to their network of colleges and universities.

In August, Crayon, Secured2 and Risk Cooperative/Ridge Global issued a press release detailing their plans to team up to combine cyber security protection and indemnification. The announcement was made at Microsoft's Government Cloud Forum in October.

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