RISK MANAGEMENT

Publication of RIMS

Can Blockchain Improve Insurance?

How Satellites Are Reducing Weather Risks

The Evolution of Parametric Insurance Coverage

RISKTECH:

The Technology Powering Risk Management

RMmagazine.com

RIMS-CRMP

RIMS-Certified Risk Management Professional

Know Risk? Show It.

Earn Your RIMS-CRMP Certification

Whether you're just starting out or on the rise, the RIMS-CRMP is a smart choice for your career. The exam covers five major areas that all risk professionals, no matter what your specialty, need to know. Earn your RIMS-CRMP to establish yourself as a strategic thinker and continuous learner who can navigate the risk environment of today and tomorrow.

Get Ready for the Exam*

RIMS-CRMP Prep Workshop

May 7–8 | Denver, CO

RIMS-CRMP Overview Course

Self-Paced | Online

** Prep courses are not a mandatory requirement for the RIMS-CRMP examination. Participation does not guarantee a passing score on the RIMS-CRMP exam.*

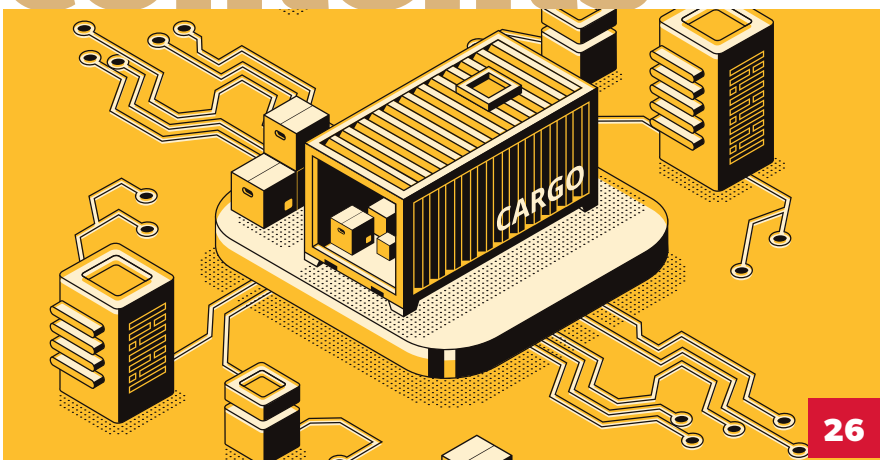
Learn more and apply at www.RIMS.org/Certification.

RIMS the risk management society

ANSI

ANSI Accredited Program
PERSONNEL CERTIFICATION
#1223

contents



COLUMNS

FEATURES

RISK MANAGEMENT

Editor in Chief
Morgan O'Rourke

Senior Editor
Hilary Tuttle

Associate Editor
Adam Jacobson

Art & Production Manager
Andrew Bass, Jr.

RIMS
The Risk and Insurance Management Society, Inc. (RIMS) is a not-for-profit organization dedicated to advancing the theory and practice of risk management.

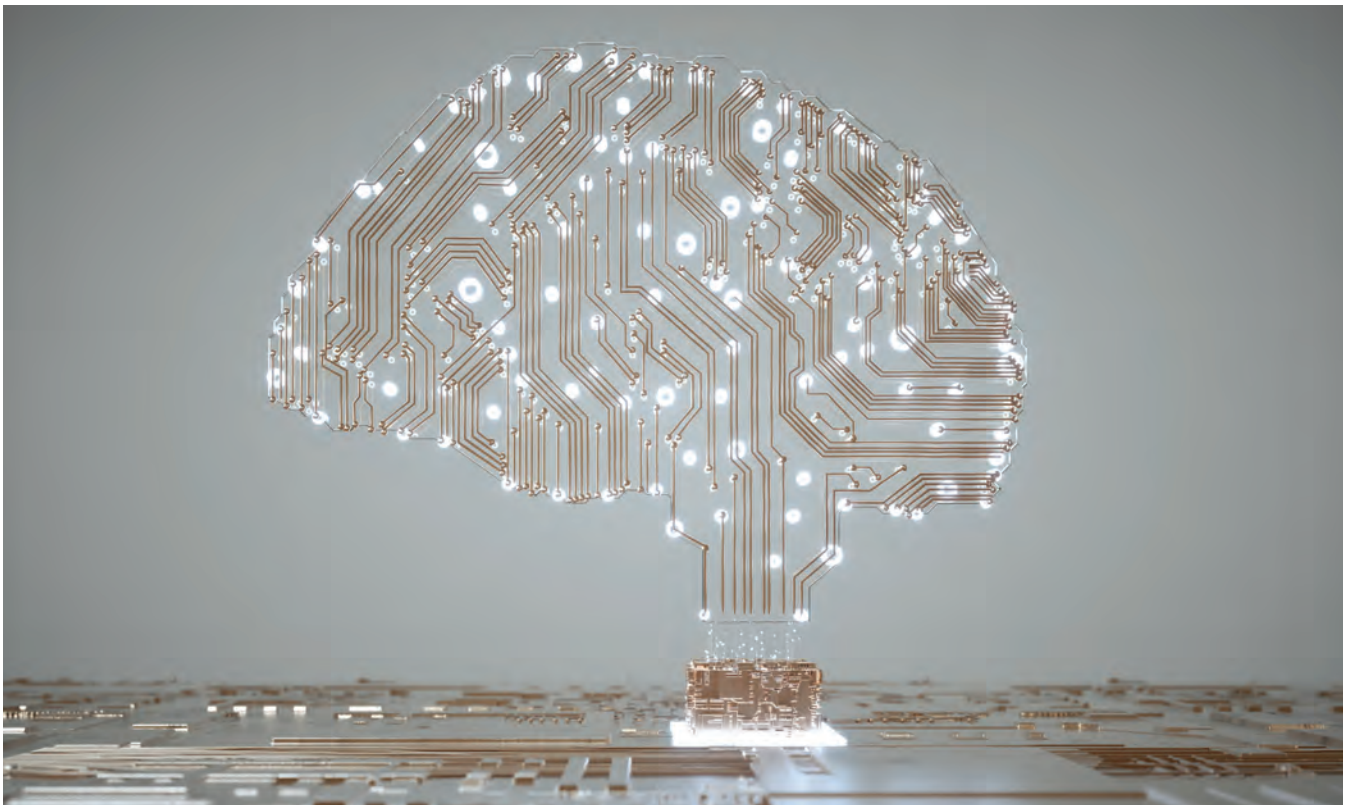
AN AWARD-WINNING PUBLICATION

AZBEE AWARDS WINNER
EXCEL AWARDS WINNER
FOLIO: EDDIES WINNER
GD:USA AWARDS WINNER

CONTACT US
All submissions and letters should be sent to:

Morgan O'Rourke
Editor in Chief
Risk Management
1407 Broadway
29th Floor
New York, NY 10018
morourke@RIMS.org
T: +1 212.655.5922
F: +1 212.655.2694

www.RMmagazine.com



Can AI Transform Compliance?

by Andrew W. Singer

Corporate compliance departments are being squeezed. Accenture's *2019 Compliance Risk Study* found that nearly three-quarters (71%) of compliance departments at financial institutions face a cost reduction target, with nearly two-thirds targeting budget reductions of 10% to 20% over the next three years. They are also suffering employee attrition, with reports of compliance officers being overworked and exhausted.

"Compliance departments have to do more with less," said Samantha Regan, global co-lead for the regulatory remediation and compliance transformation group within Accenture's finance and risk practice and co-author of the study.

Thus, there is an urgency to embrace new technologies like natural language processing (NLP) and artificial intelligence (AI) to improve compliance productivity. The study calls for "a new generation of compliance talent that is digitally fluent, well-versed in analytics, and capable of delivering proactive risk insights."

Current compliance professionals will not become redundant overnight, Regan said, as departments need to maintain a balance of skills. It is more about adding professionals with new skills, such as those trained in NLP and machine learning, who can create scoreboards, visualizations, predictive models and the like. It is about doing the same job in a different, more efficient way.

In the coming years, artificial intelligence may radically improve compli-

GETTY/ANDRIY ONUFRIYENKO

WE WANT YOU

Share your expertise and perspective with your peers and help create a stronger and more vibrant risk management community by contributing to *Risk Management*.

Visit **RMmagazine.com/contribute** for details on how you can get involved.

RISK MANAGEMENT

ance, aiding the critical shift from check-the-box toward a risk-prevention outlook—"not so much because of the cost issue, but because it will allow companies to re-imagine their processes," said Dilip Krishna, chief technology officer for Deloitte Risk and Financial Advisory.

To be sure, the speed with which NLP and other AI processes can work through a pile of documents is impressive. For example, regulatory technology firm ComplyAdvantage estimates that it can process 150 million articles a month—6.5 million articles a day—looking for the adverse media reports used in anti-money laundering (AML) compliance. By comparison, 50 traditional bank researchers working a full day without breaks can cover 24,000 articles, according to Livia Benisty, head of the firm's financial crime unit. AI processing is often more accurate, too.

In the coming years, artificial intelligence may radically improve compliance, aiding the critical shift from check-the-box toward a risk-prevention outlook.

But most noteworthy are the potential qualitative changes that AI could bring to compliance, Krishna said. Are loans being booked accurately into the bank's internal loan system and in compliance with the applicable loan regulations, for example? With traditional compliance processes, human beings might look at 10% of a bank's loans to ensure things are being done correctly, while AI processes can review 90% of the data, improving accuracy. Even more impactful, AI systems might eventually do the actual booking, eliminating the need for this kind of first-line compliance altogether.

In the meantime, the compliance costs and manpower requirements in heavily regulated industries like financial services can be daunting. The Bank Secrecy Act, for one, requires financial institutions to detect and report customers engaged in money laundering, fraud, terrorist financing and sanctions violations. In a large bank, 200 to 500 analysts can be occupied with know your customer (KYC) and AML compliance alone, scouring news articles and other public reports to avoid onboarding clients with sketchy pasts, Benisty said.

The false-positive rate in these media searches is very high, however—on the order of 95%, she said—which means following up on most searches red-flagged using a traditional rules-based search is "a complete waste of time and money." Only about 2% ever lead to a Suspicious Activity Report (SAR), she estimated.

NLP can do better because it looks for context. Traditional adverse media searches might use Google and other tools to scan the internet for hot words like "harassed," "indicted" or "charged." But words can be ambiguous. "Charged," for instance, can mean to accuse someone of an offense under law, but it can also mean to entrust someone with a task. Consider a headline like "Elizabeth Warren Charged with Reinvigorating the Democratic Caucus." A traditional search might flag that article, but an NLP process probably would not because it would also look at adjacent words in the headline like "reinvigorating," which is more often associated with the benign meaning of "charged."

Using NLP and other AI algorithms, ComplyAdvantage can reduce false positives by 70%, Benisty claimed. The financial institution can then get by with fewer analysts and reduced costs, or, alternatively, the bank's analysts can be freed up to do more meaningful work.

Regan noted AI and NLP can also be applied in non-financial sectors like trade surveillance, anti-corruption compliance (e.g., picking up violations of the Foreign Corrupt Practices Act from time and expense reports), and privacy compliance (e.g., identifying personally identifiable information violations).

NATURAL LANGUAGE GENERATION

NLP is still in the early adoption stage in organizational compliance departments, but an even newer AI technology is now emerging: natural language generation (NLG). NLG analyzes structured data and summarizes its findings using natural language. In other words, the software writes compliance narratives automatically.

"Natural language generation is great for SARs," said Anthony S. Dell, chief compliance officer at venture capital firm General Catalyst. Writing SARs is time-consuming and repetitive, and many

bank compliance officers could use that time for more strategic tasks.

According to Keelin McDonell, senior vice president at NLG technology provider Narrative Science, NLG can reduce the time spent preparing SARs by as much as 75%. The NLG report is generated almost immediately, but often a compliance officer will review the AI-generated document and may add anecdotal evidence. As institutions often write thousands of SARs a month, the annual savings to big banks from automating these processes could be in the "seven figures" range, McDonell estimated.

NLG is not yet a silver bullet, however. One common misconception is that users can input data in any form and the software will spew out fully-formed prose, but it requires clean, structured language. Some companies that attempt to implement the technology have failed to anticipate the amount of preparation required and have struggled to get NLG programs up and running.

NLG has been useful in some areas, like reporting on sports events using the structured language in a baseball box score, said John Lucker, principal at Deloitte Advisory. It might also be effective with fact-based reports, like SAR or EDGAR filings. But language is complex. Understanding sarcasm, double negatives, or idiomatic expressions is still problematic for computers. It is not clear how far NLG can be taken before its output sounds like computerese (which it is, of course). The software's lexical rules engine also often only works in English.

That said, the technology allows companies to deploy analytics to a wider audience, not just data analysts, which means organizations may not be so beholden to "expensive and hard-to-find talent like data analysts, data engineers and data scientists," according to research firm Forrester.

Overall, NLG and other machine learning technologies have a role to play because the compliance burdens faced by organizations are "not trivial," Lucker said. For instance, pharmacies are increasingly required to track prescriptions amid issues like growing public concern about opioid addiction. Most prescriptions are still paper-based, so some companies have sought to streamline the tracking process using handwriting-reading software. The technology remains a work in progress, however. Software can read about 80% of the prescriptions accurately, but human beings still have to deal with the other 20%, meaning it is not eliminating the burden, just the number of people involved in the task.

Compliance has been somewhat neglected in recent years, he noted, with few companies heavily investing in it lately. The Trump administration has been deregulating, but regulations are not necessarily being rolled back at the state level, and many of these can be quite onerous, such as the forthcoming California Consumer Privacy Act.

THE RISKS OF AI

AI comes with its own risks, of course. As the Accenture report noted, "The financial services ecosystem also continues to experience a surge of newer types of risks anchored in technology and data, such as cyber and privacy. Such risks are further compounded by the growing adoption of artificial intelligence in business processes, which presents additional ethical issues. Compliance officers may find themselves having to navigate these without the ability to foresee unintended consequences."

Last year, Amazon had to scrap an AI-based hiring tool after it demonstrated a bias against women, for instance. The company used resumes from the previous 10 years to "train" the model to select successful applicants, but as in the tech industry overall, the resumes of candidates who were hired were overwhelmingly male, so the model "learned" to select other resumes from men.

There will always be risks with black-box processes like AI, Benisty said, but there are also risks with human beings doing compliance searches. If compliance departments hire the right people who understand the technological tools and their limitations, some of those risks can be mitigated.

That said, if a suspect character tries to open a bank account and a SAR is filed with regulators, then compliance departments have to be able to explain exactly why this person's activity was deemed suspicious. At some level, the technology must be interpretable.

In five or 10 years, Dell foresees more intuitive AI-type tools. Doing advanced analytics will be like an internet search today. Dell believes "we're heading in a great direction" with respect to AI and compliance, but noted that, especially in larger organizations, "what will make the difference [in the future] is still the human element, building human relationships."

In any event, the status quo with regard to compliance is not acceptable. "We can't continue as we are going," Benisty said. "Compliance is failing." Compliance departments cannot keep up with the skyrocketing amount of financial crime, and many companies face a level of unmanaged employee attrition that is above expectation.

"The time for compliance departments to maintain the status quo or take incremental steps in the face of disruptive forces has passed," Regan said. "Financial services has changed, and compliance has to change with it." ■

Andrew W. Singer is a New York-based freelance writer.

Mitigating Construction Risk with Technology

by Dr. Donna Laquidara-Carr

Construction has always been a high-risk venture, but recent trends are exacerbating those risks, including a shortage of skilled workers and accelerated construction schedules. New developments in technology, however, may help mitigate their impact.

Today, unprecedented access to worksite activity data is available through sensors, wearables and artificial intelligence-based solutions that can help eliminate or reduce hazards. These technologies can help contractors pay more rigorous attention to risk and manage it more effectively.

In the report *Using Technology to Improve Risk Management in Construction SmartMarket Insight*, Dodge Data & Analytics and Triax Technologies examined the challenges that contractors face when managing onsite risks, the potential for technology to help address them and the role insurers can play in the wider adoption of these technologies.

"The findings from the Dodge Data & Analytics research are encouraging and confirm what we've suspected: that contractors and insurers alike see the value in leveraging IoT [internet of things] technologies to help collect, analyze and act on risk management data," said Ian Ouellette, vice president of product at Triax Technologies.

CONTRACTORS FACE ONGOING CHALLENGES

The study found managing project risk is an ongoing challenge for contractors. Just over half of those surveyed said that they face at least a medium level of difficulty identifying project risks. Being able to identify project risks is essential for assessing or managing those risks. This alone points to a serious issue in the industry, which cascades into other difficulties, including conducting ongoing management of project risks (reported by 66%) and preparing critical assessments of project risk (63%). To identify project risks, prepare critical assessments of them and manage them, contractors need better data about onsite risks, and they need it captured in a way that allows for analysis across projects. Technology can help contractors address this need.

Insurance executives interviewed for the report believed that most contractors struggle to gather sufficient data, and even fewer are able to capitalize on it. One executive said that the majority of contractors are gathering data at a very basic level, while another said, "I don't think contractors gather data to measure risk outside of risk of performance, and health and safety." However, two others noted that they have seen improvements in this area over the past five years with the advent of new technologies. The consensus from

SHUTTERSTOCK/PREECHAR BOWONKITWANCHAI

these interviews was that capabilities are growing, but that the construction industry still needs to mature in its ability to gather and analyze data to improve their risk management capabilities.

RISKS THAT TECHNOLOGY CAN ADDRESS

Technologies using sensors, commonly referred to as internet of things devices, have recently emerged as tools to manage risks onsite. Contractors said that the greatest benefit of IoT technology is in reducing occupational risks. In fact, 41% said they believed that IoT tools potentially offer a high level of improvement in occupational risks, and another 32% expected to see moderate improvement as these technologies are more widely deployed.

Addressing occupational risks is particularly important to contractors who prioritize their workers' safety and can struggle with how injuries impact their schedules, productivity and bottom line. Many contractors face skilled worker shortages, which exacerbates these impacts by making it difficult to replace injured workers quickly with qualified personnel. Also, more inexperienced workers may be learning their trade on the job, further increasing these risks. All of these factors make addressing occupational risks a top priority for contractors.

The insurance executives interviewed agreed, unanimously saying they regarded occupational risks as one of the top areas that new technologies can improve. While they did see the impact of other technologies like visual auditing and augmentation to address these risks, they too regarded IoT technology as particularly useful, and commented on the potential of wearables that track worker movements, proximity sensors on vehicles and equipment, and biometric devices that can measure exhaustion or inebriation. One executive described these types of technologies as "a game changer for the construction industry."

Another said that wearables will soon be standard operating procedure: "When you show up to work, you get issued your wearable and you go along as you've always done, but there's data being collected that will be used to mitigate risks."

Contractors and insurers alike also saw the potential for technology in general—and IoT technology in particular—to help contractors address other types of onsite risks. Over half of the contractors interviewed saw the potential for at least a medium level of improvement when deploying IoT technologies to address risks to the public/non-workers (i.e., general liability), property damage risks and construction defects, and 49% reported the same for financial risks.

Several insurers also saw strong potential in using IoT technology to address property damage and construction defect risks. Additionally, they were enthusiastic about the potential for video inspections to reduce general liability and construction defect risks, especially when combined with artificial intelligence to detect hazards. The level of enthusiasm for these technologies was particularly striking since most contractors are not currently using much of this technology.

INCREASING INVESTMENT IN RISK-REDUCING TECHNOLOGIES

However, the study revealed a major obstacle to widespread adoption: Most contractors do not have innovation budgets for these kinds of investments. Instead, they typically either absorb the costs hoping for future gains or they pass on the costs to their clients.

Two-thirds of contractors (67%) reported that negotiating lower insurance premiums was the most important factor that would encourage them to adopt risk mitigation technology. Most insurance carriers do not consider offering lower insurance premiums a possibility in the short term until they have gathered sufficient data on the degree of risk reduction.

This does not mean that insurance companies and brokerages are simply standing on the sidelines hoping contractors adopt technology, however. Most are increasing their own knowledge so they can be a resource to contractors looking to invest in the right tools. Over half (56%) of the contractors in the study agreed that their relationship with their insurance carriers was more of a partnership than a one-off transaction, and many of the insurance executives agreed with regard to technology adoption. As one executive said, "[Contractors are not] familiar with what is out there, so if we can help to raise awareness and show some value by doing something differently or using a technology tool, that might be helpful for them."

Some insurance executives also pointed out that lower deductibles are possible for proven technologies, and if the technology provides the expected benefits, fewer claims over time will result in lower premiums.

To that end, some executives reported that their companies are partnering with contractors to help fund the adoption of particularly promising technologies. For example, they have shared the initial cost to install telematics in work vehicles to track driving patterns and found that contractors see such a clear benefit that they shoulder the ongoing costs. "[Contractors] don't have time to do the due diligence. They don't have enough confidence to put the money upfront [for technology] and then manage it," one executive explained. "The implementation of technology within their businesses is where they struggle. And that's really where an insurance carrier needs to be involved if it's going to push this type of technology." ■

Dr. Donna Laquidara-Carr, Ph.D., LEED AP, is industry insights research director at Dodge Data & Analytics.

Building an EERM Toolkit

by Dan Kinsella

More enterprises are waking up to the importance of extended enterprise risk management (EERM)—the process of identifying and managing risks that come to the organization through third parties, vendors and other external sources. As the use of cloud services and other third parties continues to grow, EERM program maturity is becoming increasingly important to mitigate risks, safeguard compliance and drive business value and efficiency in the process. A Deloitte poll revealed that the majority of respondents (70%) indicated a moderate to high level of dependency on external entities that might include third, fourth or fifth parties, with nearly half (47%) of respondents saying that their organizations had experienced some sort of risk incident involving the use of external entities in the last three years.

While it is no surprise that the C-suite and board are seeing more clearly the importance of developing a mature EERM program, the path to program maturity can still be challenging. In 2018, a Deloitte Touche Tohmatsu Limited global survey on EERM revealed that only one in five responding executives say their organization has an integrated or optimized EERM program. While integrated and optimized EERM mechanisms can improve the overall maturity of these programs, the apparent maturity lag suggests that, even if enterprise leaders are sold on the why, they may feel stuck on the how.

SHUTTERSTOCK/STUDIO G, EMOJOEZ

One way to address this problem is through the use of EERM tools—technology-driven systems, applications, controls, programs and methodologies that can help enterprises achieve program maturity. By using these tools, organizations are shifting the focus from claw-back recovery efforts to ongoing, pre-invoice validation to prevent problems from occurring in the first place. Organizations that effectively utilize EERM tools stand to gain the biggest ROI from greater efficiency, better compliance and fewer risks from reputation damage, regulatory missteps, consumer backlash and cyberattacks.

PUTTING EERM INTO PRACTICE

As third-party ecosystems grow, more effectively managing the associated risks can help organizations gain competitive advantage. A recent Deloitte white paper estimates those organizations that have a good handle on their third-party business partners can outperform their peers by an additional 4% to 5% in terms of growth to their bottom line.

An EERM tool is essentially a practical lens that focuses on a specific workflow or particular piece of your enterprise operations. These tools can assess the nature and severity of risks, gauge the "materiality" of threats for prioritizing reme-

diation, and provide decision support for both tactical judgments and larger strategic business decisions that affect the whole company.

For example, cognitive technologies can cut down on labor intensive and repetitive tasks that can lead to error and inefficiency. In the past, the process of writing and revising third-party contracts has been largely manual. That can be trouble if regulatory changes—such as the EU's General Data Protection Regulation (GDPR)—force you to renegotiate many contracts en masse. Cognitive technologies such as natural language processing can help organizations automatically perform textual analyses of their third-party contracts to pick up on language that could signal areas of risk related to GDPR and flag them for closer review.

Related EERM tools include workflow improvements to consolidate the security audit process for a third-party vendor that works with more than one part of the enterprise, eliminating the need for different departments to do their own security audit on the same vendor. And in government settings, the Federal Risk and Authorization Management Program (FedRAMP) process for assessing the security of cloud services can be simplified with templates that inherit data from FedRAMP-approved cloud service providers to get rid of redundant compliance validation on applicants that rely on such services. The cloud can also play an important role in enabling third-party risk management service providers to efficiently deliver services such as vendor background checks, vendor risk monitoring, payment solutions, and the like—at a much lower cost than building and maintaining proprietary solutions.

Many organizations are already using robotic process automation (RPA) for processing invoices and conducting compliance checks; some are beginning to redeploy it to more sophisticated risk analysis. For example, critical data about external-party relationships can reside in multiple procurement systems as well as in emails, spreadsheets and text documents. Where manually consolidating this data would be prohibitively labor-intensive, RPA tools can extract, highlight and reconcile the information across multiple systems with relatively little human intervention, improving EERM efficiency and scalability.

EERM tools continue to evolve with technology. Organizations are increasingly using blockchain, for example, to create distributed digital ledgers for a "single version of the truth" to safeguard transaction records and improve clarity about risk exposures. And sensing tools can automate the due diligence of examining third parties for cyberthreats, dark web exposure, negative news coverage, financial weakness and other risk factors.

THE ROI OF EERM TOOLS

These examples underscore how EERM tools are more than just good ideas for risk reduction—they are also good ideas for ROI and value creation. Especially among board members and others in stewardship roles in the organization, the default view of risk is typically a defensive one to guard against regulatory missteps. But the ROI side of the equation is clearer as EERM tools now give organizations the ability to apply risk management precisely where it is needed. Mature cost and revenue recovery efforts can help an organization save 1% to 5% on spending, with reviews of single third parties yielding millions of dollars to the actual bottom line.

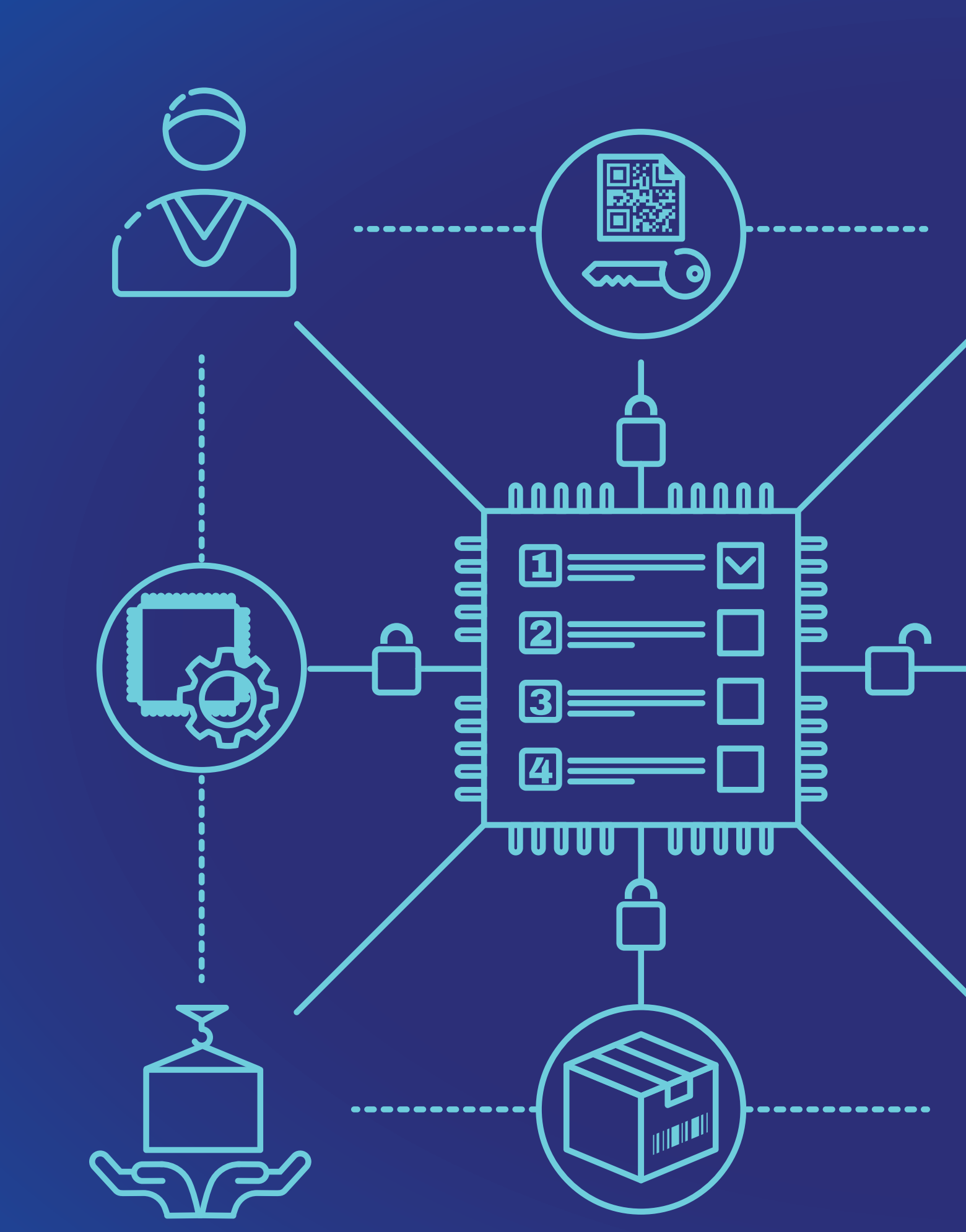
Deloitte poll respondents indicated that their organizations are likely to invest in a number of emerging technologies and tools during the next 12 months, including cloud computing, robotic process automation, data visualization, cognitive technologies, and blockchain and internet of things applications. Such tools invariably pave the way to fewer silos in the organization—a good thing for the larger EERM mission and the overall health of the company. The reason is that compliance, procurement and other EERM-related issues are common challenges that happen to be expressed in different business contexts across the enterprise. Once there is a software or workflow improvement that can help address everyone's problem, it is easier for that tool's benefits to be understood—and adopted—organization-wide for a more holistic approach to governance.

As technology improves and organizations become more aware of potential economies of scale, more collaborative platforms and third-party risk services are likely to emerge. Another approach may be to offer "shared utilities" where the risk service provider conducts standard assessments that are shared across a group of organizations.

Reducing silos around EERM also improves risk-awareness and consistency. With the help of these tools, organizations can move toward a more centralized EERM approach to aggregate insights at an organization-wide level. Some organizations are adopting a middle ground between a siloed and a fully centralized model. In this "federated" model, EERM guidelines and oversight are centralized, while process execution remains distributed. Such an approach enables organizations to not only have a cross-risk view of third-party relationships and understand concentration of risk, but still customize execution of third-party risk management to be better positioned to address unique areas of the value chain.

Regardless of the formula used, organizations are getting better at leveraging EERM tools and their adoption is likely to increase as third parties take on more mission-critical, core functions in the organization. Robust EERM programs can be costly, but their net value has been proven time and time again in terms of security, risk aversion, process improvement and hard dollar savings. ■

Dan Kinsella is a partner in the Risk and Financial Advisory practice at Deloitte & Touche LLP.



COMPOSITE BY ANDREW BASS, JR; SOURCE ART: SHUTTERSTOCK/TRIKONA

Can Blockchain Improve Insurance?

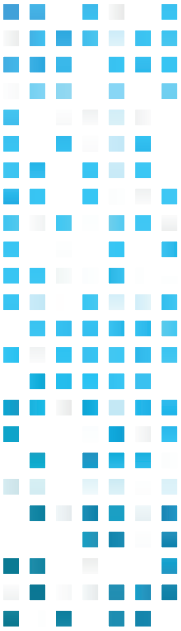
by Andrew W. Singer

FRAUDULENT CLAIMS CONTINUE TO PLAGUE the global insurance market, but proponents of blockchain technology insist that a solution may soon be at hand. When implementation of these decentralized digital ledgers becomes widespread, some believe fraud could be reduced significantly.

An estimated 5% to 10% of all insurance claims are fraudulent, costing U.S. non-health insurers more than $40 billion a year, according to a 2017 McKinsey & Company report, which suggested that "by serving as a cross-industry, distributed registry of external and customer data, blockchain can be used to identify fraud." Indeed, a 2018 Boston Consulting Group (BCG) report predicted that an "all-blockchain" auto insurer could lower its total operating ratio by 10 to 13 points compared with a traditional carrier, two points of which would be from fraud detection alone.

Others contend that new insurance markets can be accessed using blockchain technology, especially in regions that exhibit high rates of corruption, because blockchains provide more reliable alternatives to current registries. In other words, blockchains could not only increase profitability by reducing current fraud, the technology could grow revenues by tapping under-served, fraud-ridden markets.

In practice, however, reducing insurance fraud through blockchain technology may not be quite so easy. "There's this notion that technology



In practice, it is not so much that the blockchain technology hinders fraud, but that the technology makes it easier to trace, potentially making prospective bad guys think twice before stealing an identity or faking a car accident.

can solve social problems, but it is naïve to think that any technology can completely eliminate fraud," said Stephan Karpischek, CEO of Etherisc, an insurtech firm that recently built a blockchain platform for flight delay insurance. While fraud is simply a function of human nature, blockchain technology has elements that can support its detection and mitigation, which is no small thing, he said.

HOW BLOCKCHAIN WORKS

Blockchain is often misunderstood. Most frequently, it is confused with the cryptocurrency bitcoin, which is only one application for blockchain—that is, the ability to store and transfer value. Blockchain is much broader, and with the addition of smart contract technology, there are far more possibilities than just cryptocurrencies.

A blockchain is nothing more than a distributed, digital ledger. It has been compared to a dusty, leather-bound ledger in a Dickensian counting house that holds records of every key transaction, but with this distinction: The same ledger is held simultaneously on thousands of different computers (or "nodes") in multiple locations with different owners, and the moment a line is added to one ledger, it appears on all ledgers.

The blockchain can also be programmed with "smart contracts," a set of conditions recorded on the blockchain, so that transactions automatically trigger when certain conditions are met. Smart contracts can be used to automate payouts for insurance claims. For example, in the case of flight delay insurance, when a flight is delayed by a certain amount of time—say, more the two hours—it will trigger a payment under the policy.

To visualize how this might deter insurance fraud, put yourself in the shoes of a fraudster, said Karpischek. You have an encrypted identity on the Ethereum blockchain (the most widely used platform) where you are known by a 20-byte encrypted address such as "0xd2a3d9f938e13cd947ec05abc7fe734df8dd826. This maintains your anonymity under normal circumstances. But in a case of suspected fraud, the government or an insurance company could uncover your physical identity.

"If you defraud someone, the government has all the evidence," Karpischek said, because all of your transactions are recorded on the blockchain, and they cannot be erased. (They are "immutable" in the blockchain argot.) "The government has a perfect trail."

This could discourage would-be fraudsters. "It's like robbing a bank and showing your passport to the [bank's] security camera," Karpischek said. In practice, it is not so much that the blockchain technology hinders fraud, but that the technology makes it easier to trace, potentially making prospective bad guys think twice before stealing an identity or faking a car accident.

The bitcoin experience is instructive in this regard. Bitcoin was the first widely distributed blockchain application. At

the beginning, in 2009, bitcoin was used by some bad actors who traded in illicit items like drugs, weapons and stolen credit cards. Now, some of those unsavory bitcoin transactions committed years ago are being linked to criminal activity. Service firms like Elliptic have sprung up to identify illicit activities conducted through cryptocurrencies and provide actionable intelligence to financial institutions and governments.

If you are "tainted," you are marked forever, said Karpischek, and you can be refused licenses, loans, coverages or accreditations, making a blockchain's immutability a potentially huge deterrent to fraud.

WHY NOT A CENTRALIZED DATABASE?

Still, are blockchains really necessary to deter insurance fraud? Would it be more

ICON DESIGNS: SHUTTERSTOCK/KRAFTED

The Leading Reference Source For Risk Management Professionals

CONTRIBUTE YOUR DATA TO THE

RIMS BENCHMARK SURVEY

AND RECEIVE A COPY AT NO COST!

The RIMS Benchmark Survey provides a unique window into the commercial insurance market. Seen against the backdrop of industry economic data, change in TCOR offer insights into the forces at work in the insurance industry. Armed with this information, insurance buyers are better positioned to design their risk financing programs, budget insurance costs, report more effectively to senior management, and negotiate with carriers.

THE 2019 SURVEY SHOWED:

- The P/C industry had a profitable 2018.
- TCOR was higher in 2018, largely due to rising insurance rates.
- For casualty lines, higher TCOR is in part a response to a higher frequency of very large losses.
- Property TCOR rose despite a significant decrease in catastrophe losses in 2018.
- Cyber insurance remains a major success story for insurers.

The Survey is based on 16,000+ insurance and represents more than $3.95 billion in premium. What trend will we see in 2020? Submit your data now, and get your copy of the 2020 RIMS Benchmark Survey free!

WHY CONTRIBUTE? SIMPLE–THE SURVEY ANSWERS THE QUESTIONS YOU CAN'T ASK ANYWHERE ELSE:

- How does the price I'm paying compare?
- Am I buying the right amount of insurance?
- What are others buying that I'm not?
- Who's writing the most of a specific type of coverage?

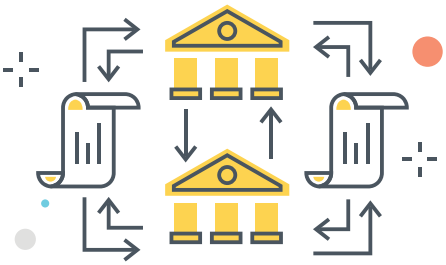
Get your questions answered. Submit your data and get your copy of the leading reference source for risk management professionals.

RIMS®
the risk management society

LEARN MORE AT WWW.RIMS.ORG/BENCHMARK

effective to put all insurance data on a single centralized database, like a national fraud registry? After all, it would run faster than a public blockchain, which needs to reproduce every transaction on tens of thousands of separate nodes.

A centralized database or registry could have positive effects on fraud reduction, said Johannes-Tobias Lorenz, senior partner at McKinsey, but there are certain advantages that are unique to the blockchain. First, a blockchain's decentralized



validation allows it to operate in situations of potential distrust, such as when it is unclear who should be the trusted party actually running the centralized database. Second, the redundancies of the distributed ledger make manipulation of data much more difficult compared with a centralized database.

The promise of blockchain technology, especially with its smart contract functionality, is that insurers no longer need to simply trust one another. "When correctly deployed, [blockchain] will enable sharing of data between insurers and other agencies," said Leanne Kemp, CEO of Everledger. "This will add significantly to each insurer's ability to combat fraud across all lines of personal and commercial insurance."

When correctly deployed, blockchain will enable sharing of data between insurers and other agencies. This will add significantly to each insurer's ability to combat fraud across all lines of personal and commercial insurance.

There are four specific areas where blockchains can make a difference in countering fraud:

1. Identity. Blockchain technology can transform the way insurance companies manage identities and personal information, said Michael Mainelli, executive chairman of Z/Yen Group. If a fraudster claims insurance benefits for a dead person, for example, the insurance company may not even know that the individual has died. If the insurer had immediate access to death certificates on a blockchain, however, the fraudster would have to ply his trade elsewhere.

2. Provenance of property and assets. Fraudulent jewelry claims alone cost the insurance industry $2 billion a year. Appraisals can be forged, appraisers and owners can collude on evaluations, and low-value jewelry can be substituted for high-value jewelry. Everledger recently built a provenance proof blockchain for the jewelry industry that tracks individual gemstones like diamonds from the mine to the end consumer, disclosing to all participants the (encrypted) identity and location of each entity involved in the stone's supply chain. Authenticating provenance is key, Kemp said, because "having transparency builds trust among stakeholders and mitigates fraud."

Everledger is also expanding into other areas, collaborating with research company True Image Solution on evaluation and restoration of cultural heritage objects on a tool that combines blockchain technology with forensic artwork reporting. "By digitally issuing and managing forensic reports encrypted on the blockchain, there is a permanent, tracked record of an artwork's authentication and certification," Kemp said. "This information can be made available—through permissioned access—to the insurance companies that require it."

3. Decentralized validation. Blockchains use validation algorithms to confirm transactions and events. This makes collaboration among insurance partners possible, even if uncertainty exists about the severity of an event. "In the case of smart contracts, for example, a claim payout would only be triggered if all nodes in the blockchain confirm a specific event, like a flight delay or a natural catastrophe," Lorenz said. "Since the nodes most likely use diverse data sources, manipulation of events becomes much more difficult."

4. Trade and logistics. Fraudulent certificates of insurance remain a big industry issue, said Mainelli. If insurance certificates were entered on a blockchain, counterfeiting scams would become less tenable.

Most agree that blockchain needs to be combined with other technologies to reduce fraud. At a minimum, this means a layer for the smart contract, but it can also

involve other things like telemetric data from a car, or the car owner's speeding tickets and car repair history, according to BCG.

THE LIMITATIONS OF BLOCKCHAIN

Blockchain is not a panacea. It will not eliminate fraud altogether. It has limitations, particularly the very big assumption that the data entered on the chain is sound.

Any software system with bad inputs will generate bad outputs. If a consignment of horse meat is falsely labeled as 100% beef, then you can track it meticulously on a blockchain all the way to the cash register at the grocery store and you still will not discover the fraud. This is the "garbage in, garbage out" conundrum, and it is particularly acute for blockchains because entries are supposed to be unalterable.

The insurance industry will not be able to dispense with fraud investigators anytime soon. One day, perhaps, a P/C carrier will be able to confirm the occurrence and severity of an event like a car crash through the multiple sensors within cars, as well as closed-circuit television and "nodes" like other cars and police reports, said Lorenz, but that is unlikely within the next five years.

"There will always be a need for investigators," Kemp said, but blockchain technology can still make a difference by identifying which transactions warrant the attention of fraud departments, while allowing legitimate claimants straight-through processing.

Scaling remains a challenge for smart-contract enabled blockchains. They cannot handle many transactions at present—too much data and transactions slow to a crawl. In a 2018 report, McKinsey predicted that blockchain is still three to five years away from feasibility at scale, "primarily because of the difficulty of resolving the 'coopetition' paradox to establish common standards." That is, natural competitors must agree on governance decisions around how the system, data and investment will be led and managed.

Some specific questions also need to be resolved with regard to governance, said Indranil Nath, vice president at DXC Technology, namely: Will systems be completely open, or will they use permissioned-based access? What are the principles for suitability in interacting with the ledger? How will information be shared among blockchain systems (also known as interoperability)?

REMOVING THE HUMAN ELEMENT

If properly applied, Mainelli believes blockchain could eventually reduce insurance fraud by as much as 20% to 40%. This assumes, of course, that the data is sound. Other experts suggest that the usefulness of blockchain is contingent on it being combined with other technologies like smart contracts, and the latest forensic approaches to stemming fraud.

Much insurance blockchain activity is currently concentrated on parametric insurance applications and catastrophe bonds, such as hurricane coverage in which a specific weather statistic like wind speeds in a certain locale can trigger a claims payment. This has certain advantages: There are no claims disputes and the data cannot be questioned as you cannot really argue with objective weather station data, Karpischek said.

While this is admittedly a small part of the overall insurance industry, perhaps it points to the real promise of blockchain—removing the human element from the claims payment process. The insurance company cannot deny you a payout if your airline flight is three hours late because the smart contract receives flight delay data directly from the air controller and a payment is triggered automatically when a delay exceeds two hours. Conversely, policyholders do not have to look for documentation to file a claim and they will be not be tempted to file a false claim. Everything will be automated. ■

Andrew W. Singer is a freelance writer based in New York City.

The Evolution of Parametric Insurance

Traditionally, parametric insurance has been used to mitigate natural catastrophe-related losses, but advances in data science and technology are creating new opportunities for such coverage.

BY ANDREW W. SINGER

Unlike traditional property coverage, parametric insurance is a type of insurance that does not indemnify the pure loss, but rather issues a set payment upon the occurrence of an objective triggering event, such as an earthquake of a certain magnitude or a hurricane of a specific intensity. Sometimes referred to as index-based insurance, this type of coverage has been around for more than 20 years, but it may now be reaching a new level of popularity as organizations look for additional alternative risk transfer options.

ILLUSTRATION COMPOSITE/ANDREW BASS, JR; SOURCE ART/SHUTTERSTOCK

One of the key virtues of such coverage is that it enables companies to deliver insurance more efficiently. With parametric insurance, you avoid lengthy claims investigations—basically, an index is triggered, a payout is made, no questions are asked, there are no disputes.

Parametric insurance is particularly effective at the country level, especially in regions like the Caribbean that are prone to natural catastrophes. For example, developed under the World Bank's technical leadership, the CCRIF SPC (formerly the Caribbean Catastrophe Risk Insurance Facility Segregated Portfolio Company) was founded in 2007 as the world's first regional fund utilizing parametric insurance to cover catastrophe-related losses. When Panama was added in January, it became the 21st member country. Each nation benefits from quick payouts even before actual damages are assessed, providing much-needed financial liquidity that is critical for recovery efforts. This was also the motivation behind the record $1.36 billion catastrophe bond issued by the World Bank last year, which relies on parametric triggers to cover earthquake risk in Chile, Colombia, Mexico and Peru.

While parametric insurance has the advantage of quicker payouts, there is one particular shortcoming: It does not cover the actual event loss, but rather the approximate loss. This introduces what is known as basis risk, where the trigger index does not perfectly correlate with the underlying risk exposure, resulting in a situation where a policyholder suffers a loss but does not receive payment. For example, a storm could destroy your building, but you will never get paid if wind speeds never reached the agreed-upon threshold. Basis risk and the potential for such shortfalls could be one of the reasons the actual amount of parametric coverage written to date remains relatively small.

The market may be changing, however. Advances in data science, sensor technology and artificial intelligence have allowed for the creation of a broader assortment of informational indexes, opening the door to new applications for parametric insurance that go well beyond the traditional natural catastrophe uses. The new generation of parametric insurance solutions include protection for cities and airports in the event of terrorism, coverages for shipping and manufacturing companies when river water-levels fall, solutions for retailers in the event of reduced pedestrian traffic during transit strikes, and economic help for hotels in the event of infectious disease outbreaks.

What these new solutions have in common is that they are not protecting against direct physical damage, but rather the indirect consequences of events, including business interruption costs and loss of attraction, so they often rely on artificial intelligence to model the indexes upon which payout triggers are based.

Four recent uses of parametric insurance demonstrate some of the innovative new applications:

When the River Doesn't Flow

In January 2019, Swiss Re launched FLOW, a parametric water-level insurance product designed to protect companies from the financial impact of high or low river water levels. The direct physical effects of low water levels are almost non-existent, but the indirect costs to businesses that depend on rivers can be significant.

There are many companies located on rivers that count on goods to be delivered by water, explained Thomas Keist, head of marketing innovative risk solutions EMEA at Swiss Re. If water levels decline, as in the warm, dry summer of 2018 in Europe, the first thing that happens is that ships can only be partially loaded since there is not enough draft (the distance from the waterline to the bottom of the ship's hull) for them to be loaded to capacity. This means they have to travel the same way twice in order to make a full delivery, which adds to the expense. If water levels sink further, ship traffic may halt entirely. Without delivery of raw goods, a factory may have to shut down.

The program uses an index formula that references measured water levels at defined river gauges. FLOW agrees to pay the company a fixed amount for each day the index remains below the defined index threshold value. Factors that determine the payout amounts are the increased costs of operation, additional expenses to mitigate the situation, and expenses not covered by traditional insurance policies. No loss investigations or adjudication are required.

Epidemic and Pandemic Protection

In 2018, Marsh collaborated with Munich Re and epidemic risk modeling firm Metabiota to create PathogenRX, a parametric insurance product designed to protect against the economic impact of infectious disease outbreaks. The product was designed for industries "that depend on people to show up," like hotels and sporting events, said Christian Ryan, U.S. hospitality, sports and entertainment leader at Marsh. If public anxiety over an outbreak of Zika or Ebola keeps people away, those businesses can fail, and often do so quickly.

The product uses a pathogen sentiment index developed by Metabiota that gauges public fear and behavioral change in the wake of an epidemic outbreak. According to Metabiota CEO Bill Rossi, the index was made possible by advances in disease tracking and reporting, software machine learning and artificial intelligence.

Alerts by health authorities and fatality counts can also be used to measure the size of an outbreak. "With PathogenRX, we are pushing the boundaries of insurability," Kraut said. "On this basis, risk layering within the policy structures is possible, which helps to achieve attractive risk premiums. The economic loss resulting from the epidemic event, however, is typically indemnified." In this sense, it is actually a hybrid parametric insurance solution.

Indexing Income Streams

In November 2018, Aon launched a new non-damage business interruption (NDBI) cover designed to protect the income streams of companies with large amounts of intangible assets, such as Uber or Airbnb. The product was developed to respond to events like terrorist threats, cyberattacks, transit strikes or

inclement weather that do not necessarily cause physical damage, but that can have cash-flow impacts on businesses like hotels, retailers and transportation companies.

Hotel data benchmarking and analytics firm STR Global developed the index, which makes use of advanced data and analytics. If a hotel's revenue per available room (RevPAR) metric falls below a certain threshold, for example, then a payout is triggered. The only exceptions are mismanagement or insolvency. Swiss Re and Lloyd's of London are providing capacity for the product.

Public Sector Terrorism Plus, which insures against acts of terrorism occurring anywhere within the borders of a public entity—or within a radius of 10, 25 or more miles—that cause a loss of tax revenue or extra expense. If the attack occurs anywhere within the radius chosen by the insured, coverage is triggered. Capacity is provided by specialty insurers within Lloyd's syndicates.

Challenges and Opportunities

In the future, as more data is collected about how people interact, parametric insurance could cover many more forms of risks due to non-physical-damage, including reputation risk. Insurers could measure if a client was caught in a social media "storm," for example, through the use of machine learning techniques like sentiment analysis. If a sentiment index reached a certain negative level, a predefined payout could be triggered.

Challenges remain, however. The basis risk challenge is not going away quickly, but to mitigate it, the current generation of parametric insurance products often uses double-trigger events or staggered payout structures that allow for partial payouts for a lower category storm and progressively higher payouts for stronger storms.

Finding trustworthy third-party reporting agencies (also called independent arbiters or "oracles") can also be difficult, particularly when operating in the developing world, said Christopher Sheehan, CEO of WorldCover. The National Weather Service might be a good "source of truth" when confirming a hurricane event in the United States, but determining drought conditions in Ghana could be more challenging. Can you really trust the local weather station using rain gauges as an "oracle"? Or do you go with a meteorological and environment-monitoring satellite service that measures soil moisture from outer space, but that may be more expensive to use?

Another obstacle to the expansion of parametric insurance is the lack of awareness and understanding among prospective policyholders. Insurers will need to convince risk managers that it really works as advertised. For example, Cripps said that he needs to talk to a NDBI prospect an average of five times before moving to the "quote" phase, while fewer meetings are required for non-parametric products. According to Matt Junge, head of property solutions for the United States and Canada at Swiss Re, parametric insurance may be an easier sell in non-corporate arenas. "In government and NGOs, it could be important in building resilience—it's a really good solution," he said. "With individual businesses, it becomes harder because you need to raise awareness about the product."

Parametric insurance has other limitations, including that it is hard to see how it can be widely applied to casualty insurance, Keist said. And it will not necessarily be cheaper to buy than indemnification coverage.

But even if parametric insurance is purchased to supplement, rather than replace, conventional indemnity insurance, it can be a useful tool in the risk manager's toolbox because payouts will be faster, with no gray areas, costly court disputes or lengthy waiting periods while a loss is confirmed. Just as many of today's most innovative technologies and services have taken advantage of improvements in data science to help streamline a wide range of traditional processes, parametric coverage can provide a more efficient insurance product, making it an equally fitting option for the modern age. ■

Advances in data science, sensor technology and artificial intelligence have allowed for the creation of a broader assortment of informational indexes, opening the door to new applications for parametric insurance that go well beyond the traditional natural catastrophe uses.

Aon may soon be working with retailers as well, using an index developed by Springboard, a firm that measures pedestrian traffic, or "footfall." For instance, after a bogus terror report last year, high-end London retailers suffered a £3 million uncovered loss in a single day, said Kurt Cripps, head of Aon's Innovation and Solutions team (UK).

The Indirect Cost of Terrorism

"The face of terrorism has changed," said Joey Sylvester, regional director of specialty programs at Gallagher. It is no longer about a building being blown up anymore, but rather people driving cars through crowds of pedestrians. Few of the buildings in the vicinity of the 2013 Boston Marathon bombing were directly damaged, he noted, but all the buildings had to shut down for a significant period.

Since there was no product to cover what had happened, Gallagher created

Andrew W. Singer is a freelance writer based in New York City.

MINI METEOROLOGISTS

How Innovations in Satellite Technology Are Reducing Weather Risks

BY WILLIAM HOSACK

GETTY/VICTOR HABBICK VISIONS

"Even with all our technology and the inventions that make modern life so much easier than it once was, it takes just one big natural disaster to wipe all that away and remind us that, here on Earth, we're still at the mercy of nature."

–NEIL DEGRASSE TYSON, *ASTROPHYSICIST*

IN RECENT YEARS, WE HAVE WITNESSED A TECHNOLOGICAL revolution that is historic, impressive and even a bit overwhelming. From the introduction of smartphones to cloud computing to artificial intelligence, the frenetic pace of innovation has led to efficiencies that never before seemed possible. For businesses, the access to information is equally profound. Accurate and timely data facilitates sound decisions in terms of protecting assets, mitigating loss and meeting fiduciary responsibilities.

The technology sector clearly understands this need, and has responded by creating whole new communities comprising data scientists, programmers, software engineers and mathematicians. They collaborate feverishly to deliver data products that can satisfy the enterprise's insatiable appetite for timely and accurate information. In some instances, inroads have been made. But in other areas, like the delivery of reliable and timely weather information, they have fallen short. The difficulty lies in the adage that the data is only as good as the source it comes from. And in this instance, the data sources—the large institutional government-based weather satellites—are fast becoming inadequate in the real-time world where businesses and rik managers must operate.

THE LARGE SATELLITE CONUNDRUM

The problem with the handful of large weather satellites that continue to orbit the globe is not that they are poorly engineered or inherently bad; in fact, it is quite the opposite. Exclusively built by government agencies, weather satellites have been designed to last nearly two decades, conduct dozens of activities, and offer exquisite scientific outputs. But these requirements drive up the size, mass and cost of these satellites. It is this last issue—cost—that has made the current model for weather data acquisition insufficient for the commercial world's needs. Many of these legacy satellites cost over $1.5 billion to build and launch, and as a result, there are very few of them in orbit. This limited number of large satellites in orbit can record and deliver data covering the world's population centers every three to 12 hours, depending on the type of observation conducted. In areas that are considered less developed—such as Africa or Southeast Asia—weather data can be even more sporadic, with observation intervals stretched to as much as every 24 hours.

This lag in reliable weather data hampers businesses by severely limiting the resources they have available to make sound decisions. Hours-old weather information is of little use to airlines that must route flights, or maritime operators that are on tight schedules to transport freight and meet strict customer demands. It also hampers farmers who must plan planting, harvesting and selling strategies in alignment with weather to maximize yields.

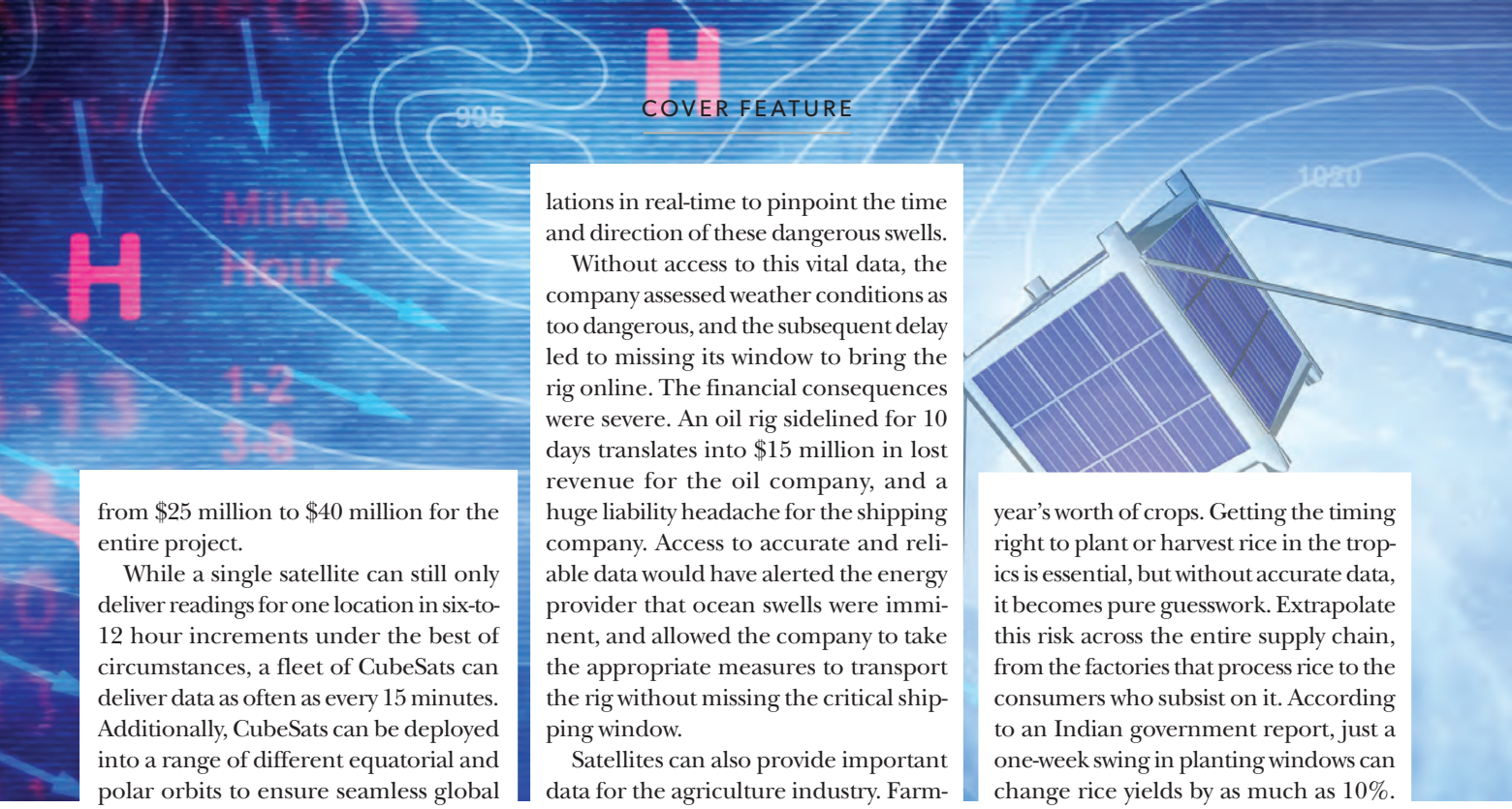
There are financial issues related to legacy satellites as well. Governments that can afford them are increasingly unwilling to invest in replacement technology. Some government agencies, such as those in the United States, United Kingdom and European Union, have begun to show a desire to rely on the commercial sector to create solutions that drive down cost while improving performance and efficiency.

ENTER CUBESATS

The business community has responded to the challenge by developing new satellite technology. While legacy satellites can be as large as a school bus, these new satellites—known as CubeSats—can be as small as a loaf of bread. Although they may seem to lack in size, they more than measure up in productivity and efficiency. Complementing the smaller satellites have been innovations in the miniaturization of instruments that enable these satellites to record and transmit vast swaths of data to a hungry market in near real-time. The variety of earth observation technologies being deployed is wide, but when looking for timely and accurate weather information, some are more effective than others.

Microwave radiometry features enable CubeSats to gather weather data through clouds all the way to the ground, which is something that other satellite-based technologies cannot do. Other observation technologies such as visual imagery are ineffective over clouds, which presents a real problem when attempting to accurately gauge conditions during even moderate weather events, let alone a Category 5 hurricane.

The economics of CubeSats also pose another notable advantage over legacy satellites. A large legacy satellite can cost $1.5 billion to $3 billion or more from design to launch. Of course, these large systems carry multiple instruments and are designed for 15- to 20-year service lives—factors that contribute to the price tag. But there are only a handful of governments that have the financial wherewithal to absorb those costs, and even if they do, the scope of observation is not substantially improved. The laws of physics still dictate the territory that one satellite can cover in a defined period. By contrast, the cost of a fleet of CubeSats—which can number from 20 to 36 in a small constellation—ranges



from $25 million to $40 million for the entire project.

While a single satellite can still only deliver readings for one location in six-to-12 hour increments under the best of circumstances, a fleet of CubeSats can deliver data as often as every 15 minutes. Additionally, CubeSats can be deployed into a range of different equatorial and polar orbits to ensure seamless global coverage. In areas that have been traditionally neglected by the large satellite operators, such as most of South America, Asia and Africa, businesses can access reliable weather data that may have a significant impact on their ability to manage risk in these regions.

TANGIBLE RISK MANAGEMENT SOLUTIONS

While the economics supporting CubeSats could certainly be attractive for a range of businesses, for several industries like energy, agriculture and aviation, access to real-time weather information can mean the difference between safe, profitable operations and catastrophe.

For example, an energy provider in Northern Europe was recently confronted by unexpected ocean swells that delayed the transport of an oil rig to its drilling location in the North Sea. The swells were higher than operational thresholds allow, and came to shore 18 hours earlier than forecasted. While the weather data that the energy company received was from one of the more established and respected government-run weather bureaus in the world, the agency was unfortunately at the mercy of the satellites and sensors gathering the data. It lacked the advanced radiometry that would accurately gauge wind, temperature and moisture, and conduct calculations in real-time to pinpoint the time and direction of these dangerous swells.

Without access to this vital data, the company assessed weather conditions as too dangerous, and the subsequent delay led to missing its window to bring the rig online. The financial consequences were severe. An oil rig sidelined for 10 days translates into $15 million in lost revenue for the oil company, and a huge liability headache for the shipping company. Access to accurate and reliable data would have alerted the energy provider that ocean swells were imminent, and allowed the company to take the appropriate measures to transport the rig without missing the critical shipping window.

Satellites can also provide important data for the agriculture industry. Farming today involves a complex ecosystem that can span the global supply chain. From growing crops to raising livestock to producing and processing to retailing and consumer purchasing down-market, weather affects businesses in any number of ways. Without good weather data, businesses have little visibility into the key factors that affect productivity, like irrigation issues, soil moisture and projecting planting and harvest windows. Further, issues relating to commodity market fluctuations, time-to-market pressures, credit and finance, and regulatory compliance must also be taken into account.

Consider a rice farmer in Northern Thailand. The weather factors that go into producing this commodity are staggering: heavy rains can occur during planting or harvest, and excessive amounts of moisture can destroy a year's worth of crops. Getting the timing right to plant or harvest rice in the tropics is essential, but without accurate data, it becomes pure guesswork. Extrapolate this risk across the entire supply chain, from the factories that process rice to the consumers who subsist on it. According to an Indian government report, just a one-week swing in planting windows can change rice yields by as much as 10%. The risk is hardly theoretical—low rice yields have caused economic depressions in a number of Asian countries.

The lack of reliable weather data is magnified further in countries like Thailand, which has historically been neglected by satellite coverage. CubeSats that can be programmed to observe these regions are a cost-effective way to mitigate risk. By increasing observational revisits and using improved radiometry to obtain better data, farmers, banks and government officials—and all participants in the agriculture ecosystem—have much better visibility into weather conditions and can make the necessary decisions to manage their portfolios accordingly.

In aviation, access to better weather data will make a marked improvement in economics, performance and safety. Better weather data means better flight planning, which allows for less head winds, optimal altitudes, fewer delays and happier passengers. From an operations perspective, avoiding turbulence and storms can decrease or eliminate the need to pull aircraft from service for additional maintenance and inspections dictated by regulations after experiencing moderate to severe turbulence.

This data is especially helpful in transoceanic flights. Even in an age with GPS, satellite imagery and reliable radio communications, an intercontinental

SHUTTERSTOCK

flight often relies on a lot of guesswork when weather is concerned. The issue is that real-time ground radar is non-existent for oceanic flights. Flight dispatchers and pilots must rely on weather forecasts that may be delivered a few hours before a scheduled departure. For a flight from Atlanta to Tokyo, for example, the aircraft may not reach trans-Pacific airspace for five hours after take-off.

Particularly in a jet-stream-fueled environment, weather conditions can deteriorate quickly. An illustration of how hazardous oceanic flight can be occurred in June 2009, when Air France Flight 447 en route from Rio de Janeiro to Paris flew through the heart of a tropical thunderstorm. The storm formed well after the pilots received their weather briefings on the ground. According to a report from the Brazilian government, the pilots were over the Atlantic and unaware of the changing conditions when they flew blindly through the storm. Ice crystals formed, disconnecting the autopilot and putting into motion a cataclysmic series of events that caused the plane to crash, killing all 228 passengers and crew on board. If better weather data was available during the flight, disaster may have been averted.

> WHILE LEGACY SATELLITES CAN BE AS LARGE AS A SCHOOL BUS, THESE NEW SATELLITES—KNOWN AS CUBESATS—CAN BE AS SMALL AS A LOAF OF BREAD.

Managing risk is predicated on evaluating sound, reliable and time-sensitive data. As legacy satellites are complemented by fleets of commercially viable CubeSats that have better resolution, expanded coverage areas and faster data processing, businesses will be able to make much better decisions to minimize the impact of weather on their operations, resources and products. ■

William Hosack is chief executive officer of Orbital Micro Systems.

How can RIMS support your *risk management journey?*

Facing risk challenges?

Ask questions and get answers from like-minded peers on Opis, our online community.

Need the latest information and best practices?

Keep your knowledge up to date and strengthen your company's risk management program with RIMS events and education.

Want to connect with fellow risk professionals?

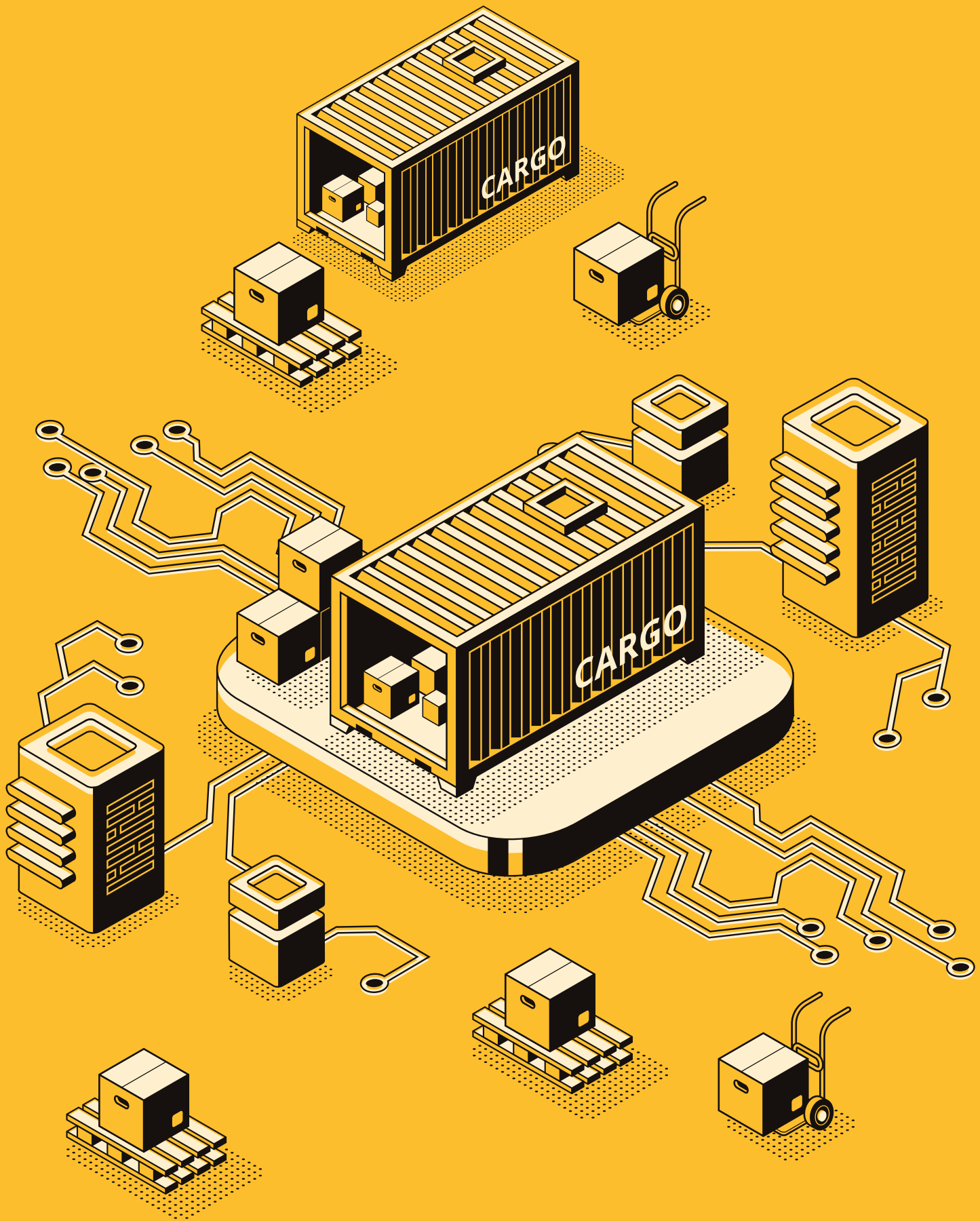
Build your local network and gain lifelong friendships when you join your local RIMS chapter.

Save $100 on RIMS membership. Complete your application and enter discount code **TECHORG100** for Organizational membership or **TECHASSOC100** for Associate membership. Offer ends December 9.*

**Offer is valid for new Organizational and Associate members who haven't been a RIMS member in at least two years. Plus applicable chapter dues.*

RIMS
the risk management society

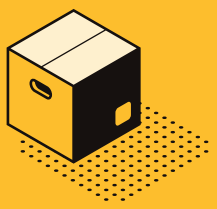
www.RIMS.org/membership



SHUTTERSTOCK/VECTORPOUCH

STRENGTHENING THE LINKS

HOW BLOCKCHAIN CAN HELP MANAGE SUPPLY CHAIN RISK



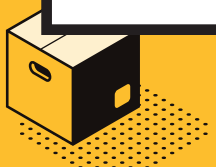
BY JOHN HINTZE

Last year, a series of foodborne illness outbreaks—including E. coli in romaine lettuce and Salmonella in eggs, breakfast cereals, raw turkey and other products—sickened hundreds of people in the United States and caused costly recalls. In response, Walmart announced in late September 2018 that it had asked suppliers of leafy green vegetables to begin implementing blockchain technology to trace their products back to the farm. The retailer had started working with IBM earlier in the year to implement the technology as part of a food safety effort. One month later, French retail giant Carrefour Group announced it would be applying the same IBM blockchain technology to track its supply chains for chickens, eggs and tomatoes, with plans to eventually deploy it across all fresh product lines.

Walmart said that with traditional paper-based ledgers typically used at many farms, packing houses and warehouses, it can take them up to seven days to track where a product came from. By applying blockchain technology, companies should be able to identify the source of contamination or other issue almost immediately. Down the line, Walmart anticipates that customers will be able to scan bags of salad and know its exact origin, potentially offering greater peace of mind.

Bühler Group, a provider of grain processing machinery used on an estimated 65% of the world's grain and 70% of its chocolate, is also implementing blockchain technology. Now in the pilot phase, the initiative aims to provide customers—grain, flour, rice and corn millers—with greater transparency about the origins of the grains they are purchasing. As consumers have become more cognizant about the source of their food, digitizing the food safety process reduces reputation and legal risk for Bühler and other participants in the supply chain, such as farmers, haulers and shopkeepers, allowing them to quickly identify and isolate sources of contamination.

Nearly one in 10 people become ill from contaminated food annually, and approximately 420,000 die as a result, according to the World Health Organization. Unsafe food also reduces productivity in low- and middle-income countries by an estimated $95 billion or more every year. With so much at stake, it is clear why more and more companies are turning to blockchain technology to help manage their supply chain risks. For companies with lengthy supply chains that span many suppliers, this application



of the technology is very attractive because it provides a highly secure and time-stamped record that is easily accessible to relevant parties and quickly auditable, ultimately helping to reduce the impact of food-borne illnesses and the scope of food recalls.

BLOCKCHAIN'S POTENTIAL

Proponents have touted blockchain technology's potential for years. Initially used for cryptocurrencies like bitcoin, a blockchain is a progression of data blocks approved by consensus and cryptographically recorded in digital ledgers held simultaneously by every participant. The chain becomes increasingly immutable as more users participate.

Supply chains would appear to be a prime candidate to use immutable records given their many risks, including counterfeit components, contamination, missing documentation, shipping delays and payment mistakes, which can result in cost overruns and potentially damaged brands. In fact, when IBM started exploring blockchain's capabilities more than four years ago, it initially decided to focus on finance and supply chain, the areas it saw as benefiting most from the technology.

The tech giant's decision to focus on supply chain was based on a "very simple intuition," according to Ramesh Gopinath, vice president of blockchain solutions at IBM. He noted that goods traveling up the supply chain, payments flowing down, and information like purchase orders and certificates of origin flowing back and forth all create inefficiencies that the "trusted information-sharing" provided by blockchain could resolve.

Many blockchain solutions used in supply chain networks today tend to have a common feature: The participants already know each other. Food producer Certified Origins, for example, has implemented Oracle's blockchain solution to ensure that counterfeit olive oil is not introduced into a supply chain that stretches from the farmers growing the olives to companies distributing the bottled oil. Similarly, Circulor uses the technology to prevent unethically sourced minerals from passing through the mining supply chain used by manufacturers of consumer electronics and electric vehicles.

The structure of such arrangements can vary by company. According to Frank Xiong, group vice president of blockchain development at Oracle, Certified Origins essentially runs its blockchain network. Another customer, CargoSmart, which manages shipment containers, instead has a consortium of ships, ports and business ecosystem participants in its blockchain. Decisions concerning the network are made collectively. Its goal is to simplify the shipping documentation process and reduce the risk of delays.

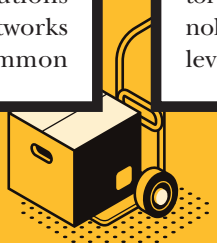
"Whether it is the enterprise-owner or consortium model, they're already in that business so they know the relevant parties and the links in the supply chain," Xiong said. Those supply chain members' familiarity with one another and the expectation that the blockchain will increase efficiency and reduce risk all facilitate the understanding and implementation of the digital ledgers, he said.

Large manufacturers, however, may not know their full network of suppliers. In industries such as aerospace, supply chain traceability has become paramount, said Andrew Stevens, research director in Gartner's supply chain technology group. Depending on the level of traceability a company seeks, it may need to connect suppliers going back three or more levels. But for a traceability solution to be completely transparent and mitigate all elements of risk in food products, he said, it would have to extend across all the levels of suppliers and the broader downstream supply-chain transactions. "I think companies have to look at the broader technology landscape and, in light of their current objectives, ask where there are other solutions that could fulfill their requirements today, which perhaps blockchain is only purporting to deliver at a certain level at this moment," Stevens added.

AUGMENTING CURRENT PRACTICES

Blockchain is relatively new technology, but many companies exploring its potential are finding that its strength often lies in enhancing existing technology. To help its corporate customers determine when and how blockchain is appropriate, enterprise software provider SAP set up the Blockchain Consortium and Co-Innovation Program nearly two years ago. It formalizes consortiums in three areas: consumer products, agriculture and retail; pharmaceutical and life sciences; and high tech. The consortiums provide SAP customers with a platform to hash out needs and priorities, and they too have concluded that blockchain's initial focus should be in the supply chain and financial functions—areas where the technology provider already provides software solutions widely used by global companies.

The Co-Innovation programs support proof-of-concept tests to gather customer feedback and eventually build a standard product to bring to market. The first such tool, launched in Decem-



ber 2018, helps pharmaceutical companies authenticate product origins before they are resold, a requirement the Federal Drug Administration will impose starting in November. A farm-to-consumer product is also in the works.

SAP already provides supply chain-related software, such as SAP Global Track and Trace and SAP Global Batch Traceability. Blockchain will be incorporated into these standard products to make supply chains more transparent and further streamline inter-company collaboration. "We're augmenting these solutions with blockchain so all the different supply-chain participants have visibility, and it's not restricted to just one company knowing where the products are," said Ganesh Wadawadigi, SAP's chief solution owner for blockchain technology for supply chains.

Ultimately, when appropriate, data collected by these existing SAP applications, and potentially also non-SAP applications, will be fed into the blockchain to be made more broadly available across the supply chain through a common user interface.

"In case of food quality issues, a manufacturer can look upstream and downstream to see where a product may need to be quarantined," Wadawadigi said. "Blockchain takes visibility and trust to a higher level whereby you can start sharing information and orchestrating business processes across companies more efficiently."

PROCEEDING WITH CAUTION

While some giants like Walmart, Carrefour and Bühler are implementing blockchain technology throughout their supply chains, some experts believe that companies still have a way to go before they can effectively implement it on a broader scale.

In fact, one of the biggest risks today may be rushing too quickly to implement the technology. Gartner research suggests the initial momentum pushing blockchain adoption has slowed as companies re-evaluate where the technology fits into their strategic roadmap and generate a more realistic view of where and how the technology can be most useful. Although there are abundant pilots, learning, exploration and development, "at this moment in time, we're not observing any robust and scalable value propositions in blockchain being applied in supply chains," Stevens said. "We talk about a five-to-10-year planning horizon in terms of accelerating the true value and positioning for blockchain as it applies to the supply chain."

Early on, organizations placed a priority on demonstrating they had a blockchain initiative, Stevens said. More recently, their analysis has extended beyond applying the technology to include issues like governance, management and culture. They have also realized that, while the technology's prospects are highly positive, there are complex and still-developing issues to be considered. As a result, companies have slowed down to figure out how to apply it most effectively for their specific circumstances.

For example, many fresh food and pharmaceutical products must be refrigerated to avoid spoilage, so it is not only important to digitally track the exchange of goods and payments between parties in the supply chain, but also the physical state of those goods, such as the temperature at which the goods are transported. Xiong said that Oracle's cloud solution can integrate technologies such as internet of things and blockchain to record the storage temperature of pharmaceutical products in a haulage portion of the supply chain.

"All these events are logged and become a permanent record, so whoever receives the items can check the record to see if a vaccine still meets qualifications or should be rejected because the shipment has crossed a safety threshold," he said.

Bühler anticipates going a step further by connecting three of its existing food safety technology systems to Microsoft Azure's cloud service, where their results will be recorded on a blockchain. These systems are designed to reduce microbial contamination in dry goods, establish a constant production flow, and improve efficiency and yield as well as traceability and transparency. The company anticipates that, in a matter of seconds rather than days, its customers will be able to see whether a food ingredient has been properly processed. It is now exploring the next steps and will most likely focus on small subsets of its supply chain because of the highly fragmented, complex stakeholders in the agricultural and food industries.

Bühler's decision to implement the technology in smaller steps fits into the paradigm Gartner sees unfolding. "We're seeing a lot about blockchain's potential in supply chains in terms of its complimentary nature, working in combination with or augmenting either innovative technology solutions or perhaps more established ones," Stevens said. "Depending on the company, the supply chain it is working across and its specific objectives, there may well be opportunities in the future, once those other technologies are deployed, for blockchain to act in a complimentary manner." ■

John Hintze is a New Jersey-based freelance writer.

10,000+ ATTENDEES

400+ EXHIBITORS

70+ COUNTRIES

300+ SPEAKERS

RIMS2020 DENVER

MAY 3-6

REGISTRATION IS OPEN

WHY SHOULD YOU ATTEND?

RIMS 2020 is the largest risk event of the year. You'll find an unprecedented number of sessions across a wide range of risk-related topics. In addition to in-depth sessions, there are shorter presentations in the Thought Leader Theater, Global Studio, Career Lab, Innovation Hub, and Wellness ZENter. Walk the Marketplace aisles to meet with your providers and discover new ones.

www.RIMS.org/RIMS2020