ventiv TECHNOLOGY

TAMING THE BLACK SWAN

The Power Behind New Risk Management Technologies

TABLE OF CONTENTS:

In a world filled with risks, there are a lot of swans out there.

Black swans. Grey swans. White swans.

Of course, we're not talking about birds. We're talking about the different types of risks -- some predictable, some not. These are all risks that are capable of bringing an organization down to its knees.

Nassim Taleb, a mathematical statistician and risk analyst, is credited for coining the term "Black Swan". His book "The Black Swan: The Impact of the Highly Improbable" focused on the extreme impact of rare and unpredictable events. He described it thus:

A black swan is a highly improbable event with three principal characteristics: it is unpredictable; it carries a massive impact; and, after the fact, we concoct an explanation that makes it appear less random, and more predictable, than it was.

For instance, the global financial crisis of 2008 would be a good example of a black swan event.

Editor's Note

Some would argue that the term Black Swan was not invented by Taleb. Instead, it is attributable to a Latin expression that means something that is highly unlikely. To put it into perspective, before the English discovered Australia, they believed all swans were white; and a black swan was impossible or non-existent.

The other two risks are more predictable:

- Grey Swan: these can be considered "long-tail risks" -- events that have a low probability of occurring but could have a potentially large cascading impact if they did. Since the threat is highly unlikely, there is a tendency for companies to ignore these risks or provide scant resources for their occurrence. (Case in point: the 9/11 attack on U.S. soil. This was due to the size of the impact and the warning signs that were ignored.)

- White Swan: these are highly predictable events that can be easily anticipated and estimated. (Taleb considers a global pandemic (like COVID-19) a white swan – "an event that is certain to occur at some point. Such pandemics are inevitable, they come because of the structure of the modern world; and their economic consequences will be even more serious as a result of increasing interconnectedness and exaggerated optimization."

When viewed after the fact, it rarely matters which swan it was -- black, grey, or white. What does matter is the damage these risks have caused, and how they could have been anticipated, addressed, or avoided.

Lessons in Risk

Let's look at some of the far-reaching risk events that have rocked industries around the globe:

Negligence: Fukushima Nuclear Disaster

Ranked as one of the largest 25 nuclear power plants in the world, the Fukushima Dai-Ichi Nuclear Power Station was constructed and operated by the Tokyo Electric Power Company back in 1971. The plant gained notoriety on March 11, 2011, when a magnitude 9.0 earthquake took place off the northeast coast of Japan. The earthquake set off a deadly tsunami with waves (up to 45-foot high) that swept over the island of Honshu and killed more than 18,000 people.

In only a three-minute timespan, the waves crashed over the protective seawall and enveloped the station. While the systems at the plant automatically shut down the reactors, the water knocked out the emergency generators which were pumping coolant around the cores to keep them from overheating. The result: the plant suffered several chemical explosions and three of the reactors had partial meltdowns. This released radioactive material into the air and forced the evacuation of hundreds of thousands of people from the region.

The Fukushima disaster is ranked as the second worst nuclear disaster (behind Chernobyl in 1986).

According to the BBC, "an independent investigation set up by Japan's parliament concluded that Fukushima was "a profoundly man-made disaster", blaming the energy company for failing to meet safety requirements or to plan for such an event."

Corporate Malfeasance: Volkswagen

Volkswagen is a German multinational automotive manufacturer headquartered in Wolfsburg. Germany. The company at one time owned 70 percent of the U.S. passenger-car diesel market, a dominance it put in jeopardy with the Dieselgate scandal of 2015.

Researchers discovered that Volkswagen was cheating on diesel-emissions by "programming some diesel-fueled cars to turn on emission controls only when being tested." These "defeat devices" were installed on more than half a million diesel cars in the U.S. and more than 10.5 million more globally to make it appear that they were fully compliant with federal emissions levels. They were not. In fact, the engines emitted far more pollution than recorded.

In the first two months of the scandal, Volkswagen lost 46% of its value. In 2016, the company announced it was eliminating 30,000 jobs worldwide. And sadly, the damages are still rolling in - to the tune of booking $35 billion of charges to earnings.

Data Breach: SolarWinds Orion

SolarWinds Corporation is an American company (based in Austin TX) that develops software for businesses to manager their networks, systems, and information technology infrastructure. In 2020, the company was the victim of one of the largest data breaches in history. SolarWinds released a software update for its Orion platform that inadvertently included hacked code. This allowed a hacker to open a "backdoor" to the system and steal information for months before someone finally discovered the leak. The company reported that up to 18,000 of its customers were vulnerable, including:

- The Department of Homeland Security
- The Department of Energy
- The National Nuclear Security Administration
- The State Department
- Microsoft and Cisco

While many of SolarWinds clients include names of companies and government agencies that fully understand the threats and vulnerabilities of cybersecurity, this breach highlighted the need for organizations to monitor the applications they use from third-party vendors.

It is important to note that Security Magazine, a leading magazine covering security news and trends, called 2020 the worst year on record for data breaches.

Regulatory Compliance: Citigroup Global Markets Limited (CGML)

CGML represents Citi's principal UK operating subsidiary, serving as an international broker-dealer and underwriter in equity and fixed income securities. In 2019, Citigroup's UK operations (which included CGML) were fined by the Prudential Regulation Authority (PRA) for failings in their regulatory reporting governance and controls. The PRA is a part of the Bank of England and is responsible for the regulation and supervision of banks, building societies, credit unions, insurers, and major investment firms.

Sam Woods, Deputy Governor for Prudential Regulation and Chief Executive Officer of the PRA reported that "Accurate regulatory returns from firms are vital for the PRA in fulfilling our role. Citi failed to deliver accurate returns and failed to meet the standards of governance and oversight of regulatory reporting which we expect of a systemically important bank."

The PRA investigation identified "the internal controls and governance arrangements which underpinned Citi's UK regulatory reporting were not in a number of respects designed, implemented or operating effectively. They were therefore inadequate to ensure accurate regulatory reporting for an organization of Citi's size, complexity, and systemic importance. This led to the significant number of errors and misstatements identified in Citi's returns."

Today's Top Risks

The list is long...and growing. Here, we highlight a few of the top threats that companies and organizations are battling every day.

Cyber Risks

Due to the increasing array of data networks, cloud deployments, and the online transfer of data (and storage), businesses are becoming increasingly vulnerable to these types of attacks.

According to a recent Accenture Cyber Threat Intelligence Report, cyber threats are increasing in frequency -- and in damaging results. Here are some of the disturbing statistics in the report:

- Five industries accounted for more than 60% of all cyberattacks in the first half of 2021: Consumer goods and services, 21%; industrial, 16%; banking 10%; travel and hospitality, 9%; and insurance, 8%.
- The insurance industry was the most frequent focus of ransomware attacks in the first half of 2021.
- Ransomware was the most frequent malware by category, accounting for 38% of attacks, followed by backdoors, which allow criminals to bypass normal authentication channels and gain remote access, which accounted for 33% of the total.

"Despite heightened awareness, government action and industry collaboration, ransomware is likely to remain one of the top threats to businesses globally," the report said. "If anything, it has entered a new phase as threat actors adopt stronger pressure tactics and capitalize on opportunistic intrusion vectors."

The average number of cyberattacks increased by 125% in the first half of 2021 alone.

The Identity Theft Research Center (ITRC), in its annual data breach report, announced that in 2021 there were a record 1,862 data compromises in the U.S., a 68 percent increase over 2020 and 23 percent over the previous all-time high of 1,506. According to the report, 294 million people had their data compromised in 2021 compared to 310 million in 2020. The report notes that ransomware-related data breaches are expected to overtake phishing as the number one root cause of data compromises in 2022 based on the current growth rate.

Business Interruption

In its 2021 Global Risk Management Survey, Aon listed business interruption as the number two risk faced by risk managers today. (This represented a dramatic departure from Aon's 2019 survey. Back then, business interruption was ranked as number seven.) To complete its top 10 risk, AON asked over 2,300 risk managers and C-suite professionals from 60 countries and/or territories and 16 industries about their key risks and how they managed and mitigated them.

The report highlighted the 1.5-mile-long Oxford Street in the West End district of London as a classic example of the effects of this risk. This shopping mecca included more than 90 flagship fashion and high-tech retail stores, restaurants, and entertainment venues. Due to the COVID-19 pandemic, the British government issued a lockdown order in March 2020 and the West End turned into a deserted and desolate area. As the pandemic began to ease, it is estimated that one-fifth of Oxford Street was closed for good and more than 50,000 retail and hospitality jobs were lost. Revenues in the district fell by more than 80 percent.

"The pandemic has subverted the traditional way we think about business interruption... It has been redefined – businesses can be interrupted on a much wider berth of issues. Because of technology and the way we do business, BI [business interruption] can be more systemic. It doesn't just happen to those in high-risk areas. BI can happen to anyone."

- Richard Waterer,
Managing Director, AON EMEA

Sadly, the effects were not restricted to just the retail industry. Business interruption became one of the top risks for the hospitality, travel, and leisure industries, as well as the energy and the life sciences sectors. The resulting economic slowdown and even slower recovery helped to exacerbate these issues. Also, it is expected that the virus will have a long-term impact on people and organizations around the globe.

Natural Catastrophes/Climate Change

Earthquakes. Floods. Wildfires. Temperature fluctuations.

It's not hard to read the news every day and not see a reference to disruptions caused by natural catastrophes and climate change. In the 17th edition of The Global Risks Report 2022 (published by the World Economic Forum), "climate action failure" was listed as the number one long-term threat to the world -- and potentially having the most severe impacts over the next decade.

The report states that "In 2020, multiple cities around the world experienced extreme temperatures not seen for years–such as a record high of 42.7°C in Madrid and a 72-year low of -19°C in Dallas, and regions like the Arctic Circle have averaged summer temperatures 10°C higher than in prior years."

The Insurance Information Institute (iii) collects information on catastrophes around the globe. In its most recent report, it stated:

- Overall losses from world-wide natural catastrophes in 2020 totaled $210 billion dollars, significantly higher than $166 billion in 2019 (according to Munich Re).
- There were 980 events that caused losses in 2020, compared with 860 events in 2019.
- Insured losses from the 2020 events totaled $82 billion, also significantly higher than $57 billion in 2019.
- Natural catastrophes in 2020 caused 8,200 deaths, compared with 9,435 in 2019.

It's only natural that people tend to think of property damage as the main challenge when it comes to natural disasters. But it is important to note that the impact goes far beyond that. It also has the potential to disrupt supply chains, company operations, the workforce and more.

Technology to the Rescue

Today's environment is complex. It's fast-moving. And it's changing at an unprecedented rate.

Businesses, organizations, and government agencies are finding it increasingly difficult to use traditional risk management models to keep pace with these changes. A deluge of data -- both structured and unstructured -- is forcing companies to adopt newer technologies to assimilate, analyze and leverage that data for better decision-making and risk assessment.

Welcome to Industry 4.0 - or better known as the Fourth Industrial Revolution.

It was the development of the steam engine in the 18th century that heralded the transition of society from an agrarian to an industrial, manufacturing-based one. This first "Industrial Revolution" gave way to the Technological Revolution in the late 19th/early 20th century -- a period where scientific discovery, standardization, and mass production dramatically transformed the manufacturing process. This was followed by the Third Revolution -- the Digital Revolution -- that started in the 1950's and witnessed the growth of electronics and computers and the sharing of information across the globe.

Klaus Schwab, author of "The Fourth Industrial Revolution" described it as "a fusion of technologies that is blurring the lines between the physical, digital, and biological spheres. There are three reasons why today's transformations represent not merely a prolongation of the Third Industrial Revolution but rather the arrival of a Fourth and distinct one: velocity, scope, and systems impact. The speed of current breakthroughs has no historical precedent. When compared with previous industrial revolutions, the Fourth is evolving at an exponential rather than a linear pace. Moreover, it is disrupting almost every industry in every country. And the breadth and depth of these changes herald the transformation of entire systems of production, management, and governance."

"The possibilities of billions of people connected by mobile devices, with unprecedented processing power, storage capacity, and access to knowledge, are unlimited," he added. "And these possibilities will be multiplied by emerging technology breakthroughs in fields such as artificial intelligence, robotics, the Internet of Things, autonomous vehicles, 3-D printing, nanotechnology, biotechnology, materials science, energy storage, and quantum computing."

According to research firm IDC, global data is expected to grow from 33 zettabytes (ZB) in 2018 to 175 ZB by 2025. It is this massive amount of data that is driving these new technologies. Let's look at some of these new innovations and how they will positively impact risk management.

Data Analytics

Data and insight go hand in hand. It is one of the reasons data analytics has been an incredibly useful tool of risk managers.

Data analytics is the process of discovering and communicating the meaningful patterns that can be found in large amounts of data. Analytics turns raw historical data into insight for making better decisions.

Data analytics utilizes historical data from multiple data sources, including emails, files, instant messages, databases, and social media to draw outcomes about the information the resides in today's companies. This historical data is then used to build a mathematical model that captures important trends.

Today, analytics help organizations establish trends, discover opportunities, and predict events or actions. While data analysis refers to reviewing data from past events for patterns; or trends, predictive analytics makes assumptions and testing on past data to produce future "what if" scenarios to help predict what will happen next, or to suggest actions to take for optimal outcomes.

Analytics relies on the application of statistics, computer programming, and operations research to quantify and gain insight into the meanings of data.

Artificial Intelligence

Artificial intelligence applies advanced analysis and logic-based techniques to interpret events, support and automate decisions, and take actions; AI applies different technologies working together to enable machines to sense, comprehend, act, and learn with human-like levels of intelligence.

In short, AI's focus is to create human-like abilities performing tasks that would normally require human abilities. It can self-correct, understand and learn. More importantly, AI analyzes data, makes assumptions, learns, and provides predictions at a scale and depth of detail that is impossible for individual human analysts.

Today, AI takes many forms. It is used in a variety of applications such as:

Speech Recognition

These AI utilize natural language processing (NLO) to transform human speech into a written format. Applications include transcription and speech-to-text translation.

Virtual Agents

Known also as Chatbots, they replace human agents with a computer-assisted customer journey -- one that can help answer frequently asked questions or provide simple, personalized advice.

Recommendation Engines

Engine algorithms are designed to effectively used by companies like Amazon, AI algorithms utilize data trends to make purchase recommendations to customers.

And AI is now expanding. For instance, many banks, insurance companies and other financial institutions are implementing AI solutions as part of their risk management processes. Using AI algorithms, these companies can now analyze and determine patterns of risk (based on past incidents) to help identify and manage potential threats, scrutinize security issues, and evaluate fraudulent activity.

The biggest challenge with AI resides with adoption. According to the research/advisory firm Gartner, only half of AI projects make it from pilot into production; those that do make it take an average of nine months to do so.

But Gartner sees that changing. “Innovations such as AI orchestration and automation platforms (AIOAPs) and model operationalization (ModelOps) are enabling reusability, scalability and governance, accelerating AI adoption and growth.”

Machine Learning (ML)

Considered a subset of artificial intelligence, machine learning can be a particularly powerful tool for prediction purposes. A key element in the burgeoning field of data science, ML uses statistical models and algorithms to sift through tons and tons of data to identify relationships or patterns that humans may not “see” or inadvertently ignore. The goal is to uncover key insights to help drive better decision making throughout the organization.

One of the key benefits of machine learning is in its ability to run a multitude of variables within the data to produce powerful predictive models. It’s heavy computing power enables it to do this thousands of times -- in split second timeframes. This enables it to “learn” from the data and enhance its predictive capabilities.

Robotic Process Automation (RPA)

This simple but powerful technology helps to perform the more mundane -- but necessary -- tasks within an organization. These software applications or “bots” are able to execute repeatable, logic-based activities to help efficiently scale business operations -- while freeing up more experienced staff for more complex problems.

Steve Culp, Managing Director of Accenture Digital Risk and Compliance, sees tremendous opportunities for RPA in the financial realm.

“In financial risk management, robotics can help identify and explain changes in risk exposure and determine data-related or business-related causes for such movement. Robotics can also be used to evaluate credit limits and determine causes for breaches in such limits, with recommendations for remedial action generated automatically.”

According to Culp, there are several areas where robotics really hits home for financial services firms. That includes regulation and compliance and financial risk management. “Robotics can help firms review employees’ disclosures regarding personal accounts and automatically examine account openings and paper statements – making employees’ trades and transfer disclosures subject to immediate and appropriate levels of review. Disclosure attestations and transfer disclosures can also be examined automatically, and robotics can reconcile employee reports on gifts and entertainment to the expense system and spot possible anomalies and potential issues."

Cognitive Computing

Move over artificial intelligence. Enter cognitive computing.

Cognitive computing is not really a new technology. Think IBM Watson, a question-answering computer system which was created back in 2007 to compete on the iconic American game show Jeopardy. If you remember, it handily beat two of the show’s greatest human champions in 2011.

Cognitive computing fuses the technologies of artificial intelligence, machine learning, neural networks, and natural language processing. While AI is designed to augment human thinking to solve complex problems, cognitive computing tries to mimic the human thought and reasoning processes. And it is programmed to learn from its mistakes.

“Companies and public sector organizations have progressed in terms of using massive amounts of internal and external data to take a more preventative risk stance,” says Samir Hans, Deloitte Advisory principal. “However, traditional methods of analysis have become increasingly incapable of handling this data volume. Instead, cognitive capabilities –including data mining, machine learning, and natural language processing–are supplanting traditional analytics and being applied against these massive data sets to help find indicators of known and unknown risks.”

Samir Hans sees fraud detection as one of the best examples for utilizing cognitive computing.

Cognitive computing is expected to grow by leaps and bounds. The market size for this next-generation computing system was valued at $8.87 billion in 2018. More importantly, it is projected to reach $87.39 billion by 2026, growing at an annual compound annual growth rate (CAGR) of 31.6% from 2019 to 2026.

What is driving this growth? According to the advisory firm Deloitte, the volume and velocity of data is what is driving cognitive computing for many applications -- including the area of risk management.

"With cognitive analytics, fraud detection models can become more robust and accurate. If a cognitive system kicks out something that it determines as potential fraud and a human determines it's not fraud because of X, Y, and Z, the computer learns from those human insights, and next time it won't send a similar detection your way. The computer is getting smarter and smarter. That's a huge game changer."

A Cautionary Note on Technology

It is easy to see that these new technologies offer immense promise for the industries across the globe. While AI is still in its infancy, McKinsey Global Institute Research estimates that AI could deliver additional economic output of $13 trillion a year by the year 2030.

But there are perils - and consequences - as well. According to Kinsey, the most visible ones include "privacy violations, discrimination, accidents, and manipulation of political systems. More concerning still are the consequences not yet known or experienced. Disastrous repercussions–including the loss of human life, if an AI medical algorithm goes wrong, or the compromise of national security, if an adversary feeds disinformation to a military AI system–are possible, and so are significant challenges for organizations, from reputational damage and revenue losses to regulatory backlash, criminal investigation, and diminished public trust."

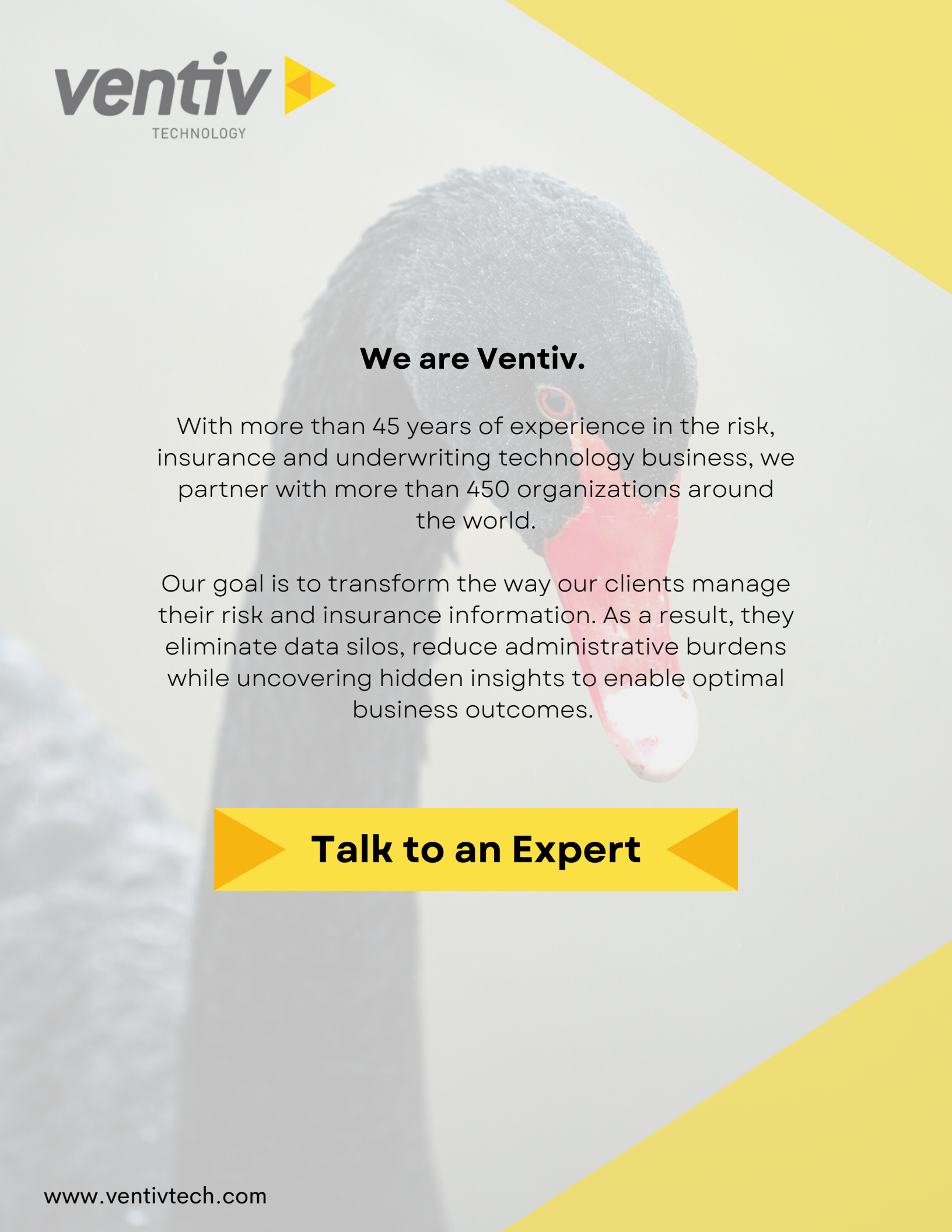
While many innovations in today's world can be considered a "two-edge sword", most risk managers argue that the benefits of using these newer technologies far outweigh the uncertainties. But they also understand that companies need to develop their own action plans to ensure that these technology risks do not become incidents to cripple their own operations.

The New Risk Management

Risk, whether it comes in the form of a white swan, grey swan, or black swan, abounds in the marketplace. And the pace of change and transformation is not slowing down.

It is the ability of today's companies - across all industries - to anticipate, weigh, and balance those risks. In that way, they can help create opportunities for innovation and growth and a competitive edge.

Today's new technologies can help. Are you positioned to leverage them to your own advantage?



We are Ventiv.

With more than 45 years of experience in the risk, insurance and underwriting technology business, we partner with more than 450 organizations around the world.

Our goal is to transform the way our clients manage their risk and insurance information. As a result, they eliminate data silos, reduce administrative burdens while uncovering hidden insights to enable optimal business outcomes.

Talk to an Expert

www.ventivtech.com