

Transformation

Caution: Safety first!

03 January 2024

Key takeaways

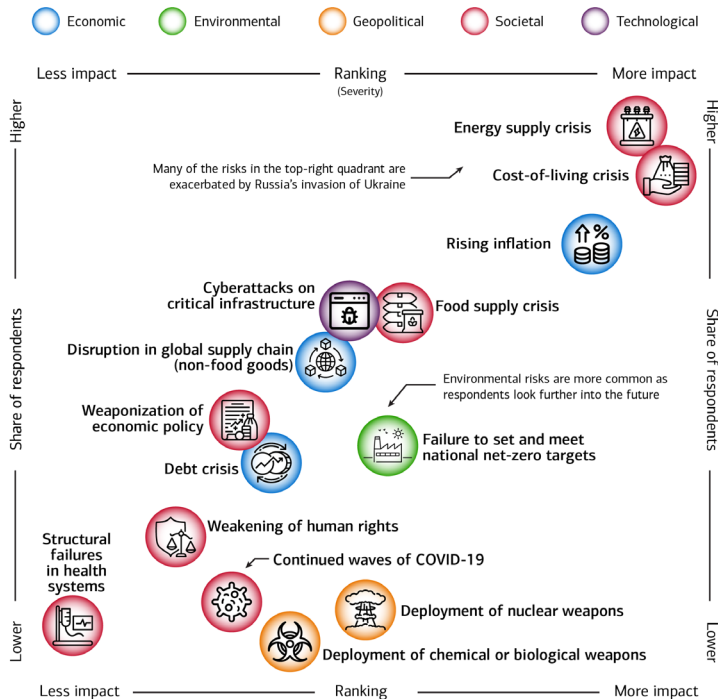
- A variety of factors contribute to why this new world feels less safe: environmental issues like climate change and extreme weather, cybercrime and deepfakes, food and energy shortages, and social polarization and inequality.
- In fact, the global risk landscape is increasingly more interconnected than ever before, and the last 30 years have seen an average of nearly 200 disasters each year, much higher than in previous decades. It's no surprise that against this unsettling backdrop, people are craving stability, safety and security.
- To address the black (or grey) swan in the room, BofA Global Research has mapped out future security solutions for a safer world that aim to address cybersecurity, cyber insurance, artificial intelligence, physical security, and automotive safety, among others.

Deep breaths

Security is like oxygen; you tend not to notice it until you begin to lose it, but once that occurs, there is nothing else that you will think about – so says Harvard University Professor Joseph Nye. The oxygen certainly feels in short supply as we move from one crisis to another – from COVID to the cost-of-living, to the climate crisis and more (Exhibit 1), which understandably makes us feel as though we are living in a more unstable world than ever before, heightening our desire for greater safety.

Exhibit 1: Top global risks in 2023

Top risks are related to issues that impact a wide variety of people, such as the rising cost of living and inflation



Source: World Economic Forum, Global Risks Report 2023, Visual Capitalist

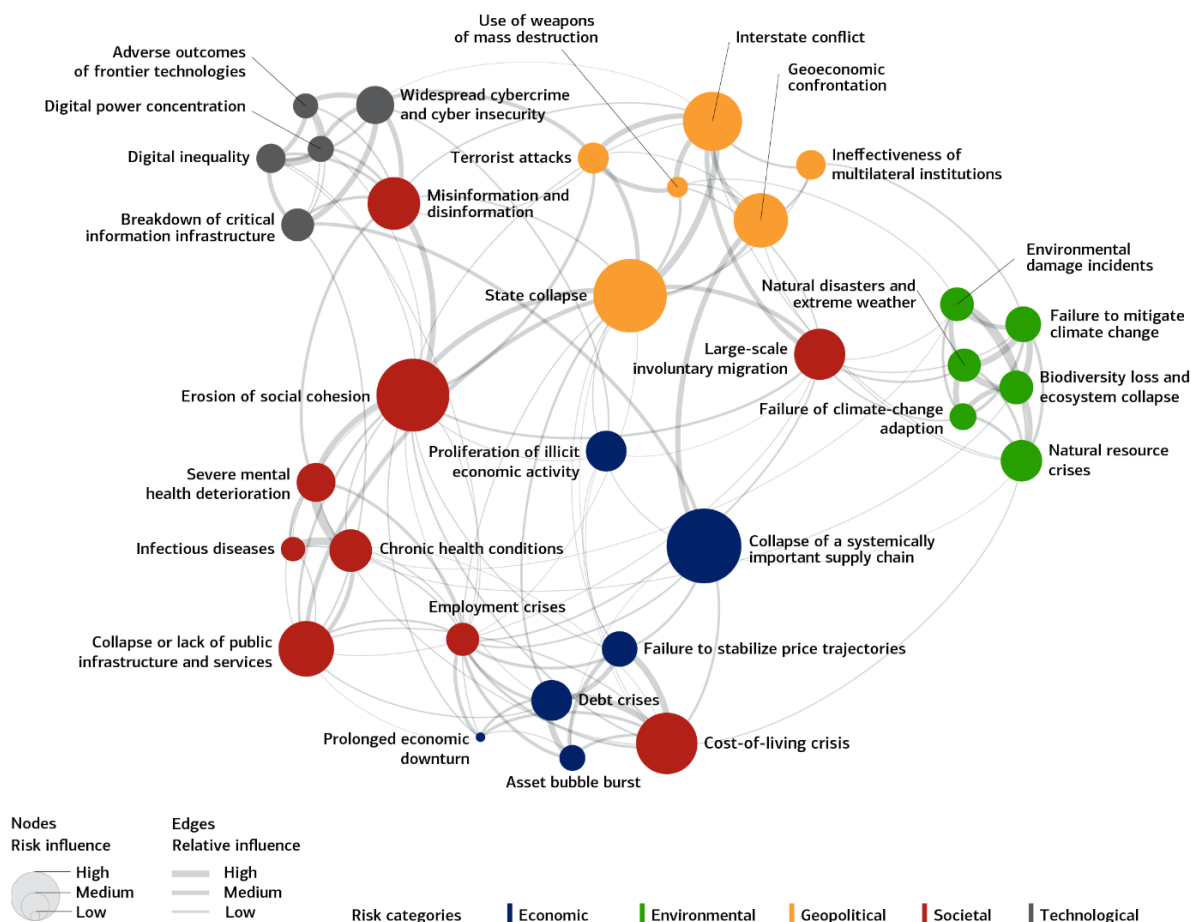
We are now living in the era of “permacrises” and “polycrises” (Exhibit 2). In fact, Collins Dictionary’s 2022 word of the year was “permacrisis,” which is defined as an extended period of instability and insecurity: a term that embodies the sense of lurching from one unprecedented event to another (Brexit, COVID, climate disasters, inflation, cost of living etc.).

Meanwhile, present and future risks are increasingly interacting with each other to form a perfect storm of “polycrises” – a cluster of related global risks with compounding effects – so that the overall impact exceeds the sum of each part. Such polycrises can arise from simple shortages in natural resources such as food, water, and metals and minerals, illustrating the associated socioeconomic and environmental fallout are interlinked (source: World Economic Forum (WEF)).

From environmental issues like climate change and extreme weather, to cybercrime and deepfakes – and from food and energy shortages to social polarization and inequality – the new world feels less safe. In fact, the global risk landscape is increasingly more interconnected than ever before, and the last 30 years have seen an average of nearly 200 simultaneous disasters each year, much higher than in previous decades. But while the world around us is transforming faster than ever, with rapid technological, environmental and demographic change – such change brings new threats and it’s no surprise that against this unsettling backdrop, people are craving stability, safety and security.

Exhibit 2: The interconnection of global risks

From polycrises to permacrises



Source: World Economic Forum, Global Risks Perception Survey 2022-23

The good news: “Safe” solutions are out there

BofA Global Research has mapped out several future security solutions for a safer world, and they include:

- **Artificial Intelligence (AI)/Cybersecurity**, which can provide solutions to the ever-growing risks of hacks. In fact, using AI automation can reduce the time to identify a cyberattack by 100 days (source: IBM).
- **Cyber Insurance** demand should see market premiums rise to more than \$33 billion by ~2027 (from \$12 billion in 2022), according to BofA Global Research.
- **Physical Safety** solutions such as testing, inspection and certification (TIC) can help with fire prevention and building/workplace safety against a backdrop of rising regulation.
- **AutoTech (automotive technology)** like advanced driver-assistance safety (ADAS) and autonomous vehicles (Avs) can reduce car fatalities.

- **AgTech (agriculture technology) solutions** can help tackle food insecurity.

The issue: Techlash from AI

Living in a connected world comes at a high price. Everything from AI job automation, the rise of fake news and the spread of misinformation through deepfake content is making citizens more anxious about the risks and threats of technology (Exhibit 3). In fact, the number of accepted submissions to FaccT (Fairness, Accountability, and Transparency), a leading AI ethics conference, has more than doubled since 2021 and increased by a factor of 10x since 2018.

BofA Global Research argues that enhanced AI/tech regulation is inevitable to protect against privacy data breaches and copyright infringement and to improve content verification. For example, starting in December 2023 most US public companies will be required to report significant hacks to the SEC in an 8-K form within four days of a material data breach.

Technology reliance

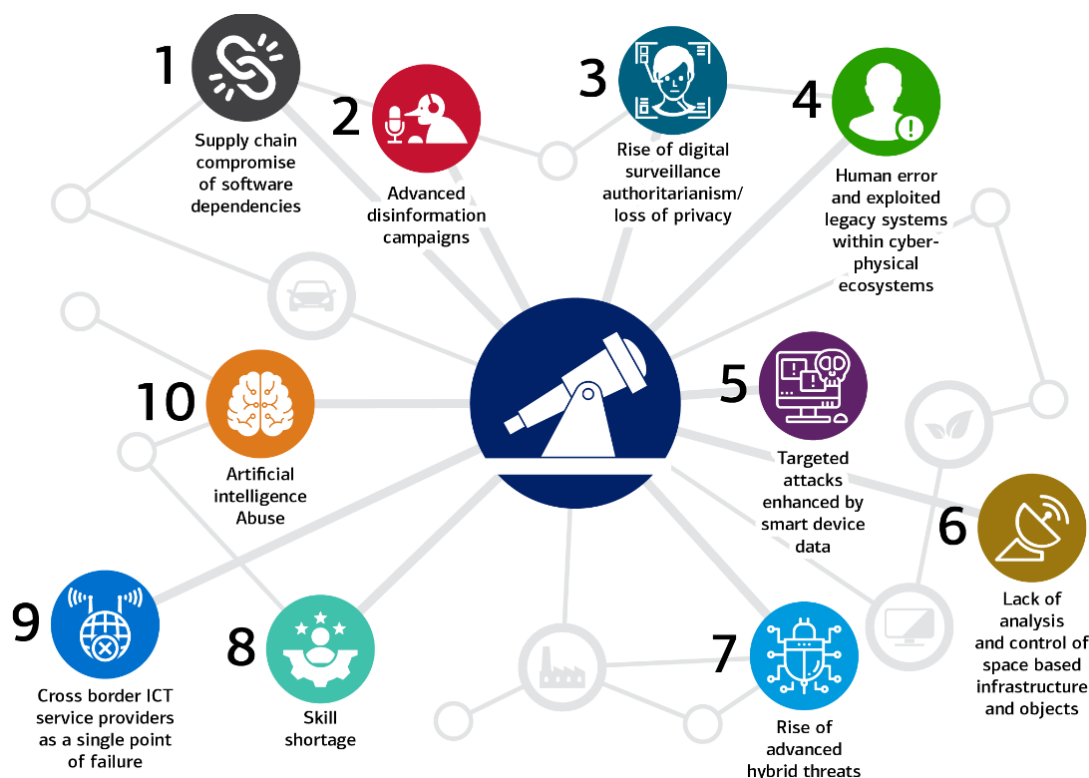
According to BofA Global Research, cybersecurity is the number one risk in a Transforming World because of how reliant we are on technology. Think about it: would it have been possible to navigate through COVID and pandemic-era lockdowns and social distancing without access to the digital world?

The rise of Generative AI creates a new menacing “threatscape.” For example, using the 10,000+ A100 Nvidia GPUs (graphics processing units) that were used to train ChatGPT, it would take around one second to crack a password today (source: NetSec, Hive Systems). And worryingly, 91% of people know the risks of reusing passwords across their online accounts, but 66% do so anyway, perhaps not realizing that hacks now take an average of 277 days (or about 9 months) to identify and contain.

The cyber threat is exacerbated by national security and critical infrastructure becoming more vulnerable to attacks. And cyber will be a key issue for corporates moving forward: by 2026, 30% of large companies will have publicly shared their cyber goals (versus less than 2% in 2021). See [Cybersecurity: Landscape, Impact and what comes next for more](#).

Exhibit 3: Top 10 emerging cyber-security threats for 2030

From supply chain compromise of software dependencies to Artificial Intelligence abuse



Source: ENISA (European Union Agency for Cybersecurity) Foresight exercise 2022

The costs of cybercrime

Another reason why this matters? According to BofA Global research, cyberattacks will cost the global economy \$8 trillion in 2023, equating to nearly \$255,000 every second, and set to hit \$10.5 trillion by ~2025, making it the world’s third largest ‘economy’ behind only the US and China. The current annual cybersecurity market spend is estimated to be \$150-250 billion, which implies cyber economic damage cost is 10x the size of cyber spend on solutions. Overall, the average cost of a data breach reached a record high \$4.45 million in 2023 compared to \$4.35 million in 2022, with the healthcare sector coming out

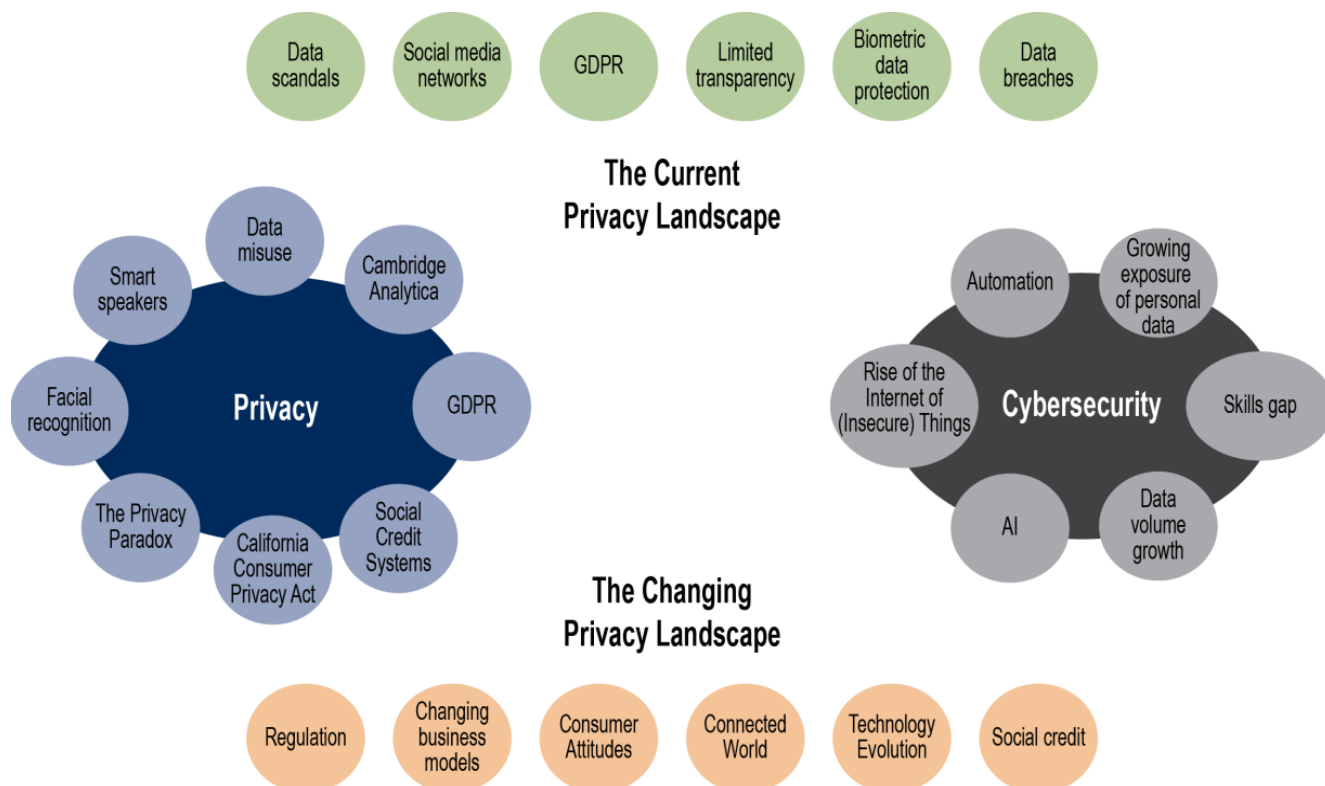
highest at \$10.93 million. And the cost of ransomware has increased from an average of approximately \$115,000 in 2019 to around \$570,000 in 2021.

Privacy, please

Privacy is not the same as cybersecurity as our personal data and digital identity become less protected (Exhibit 4). In fact, 99.98% of US residents could be correctly reidentified in any data set, including those that are heavily sampled and anonymized using just 15 demographic attributes. What’s more, 90% of personal data will require protection, but only half will have it by 2025. As a result, a combination of regulation, e.g., the European Union’s General Data Processing Regulation (GDPR) and the California Consumer Privacy Act (CCPA), and consumer awareness on online safety will be critical to safeguarding privacy. For instance, 65% of the world’s population will have personal data covered under modern privacy regulations by 2023, up from 10% in 2020. And today 86% of internet users have tried to be anonymous online and taken at least one step to mask their behavior or avoid being tracked.

Exhibit 4: Privacy versus cybersecurity

Landscape comparison of between privacy and cybersecurity



Source: BofA Global Research

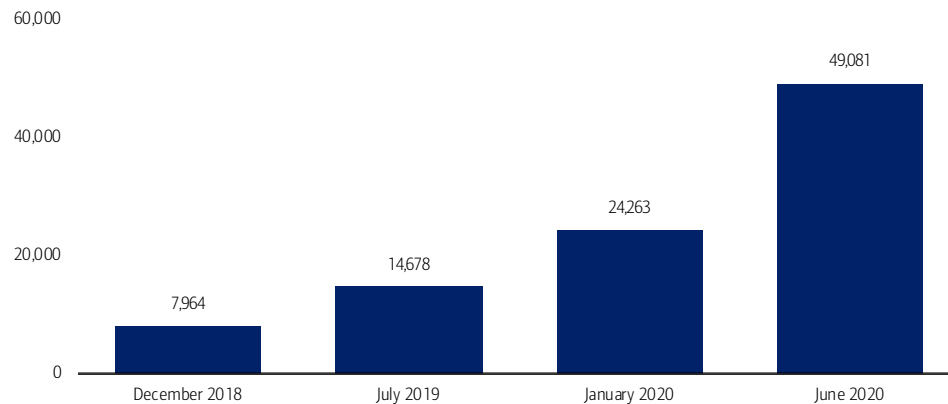
Faking it

Fake news is false or misleading information that is presented as news. It could be forms of misinformation (where false information is shared by accident without intent to cause harm) or disinformation (where false information is shared to deliberately mislead and cause harm). Regardless, fake news creates distrust and undermines the truth. Yet, young people tend to view misinformation as less worrisome than their older counterparts – a finding that aligns with previous research showing that young people are less likely to share misinformation online and have more confidence in navigating falsehoods on social media (source: Pew Research).

Meanwhile, as discussed in [When seeing is no longer believing: the dangers of deepfakes](#), deepfakes are a type of synthetically modified media used to impersonate real humans, and are one of the most effective and dangerous tools of disinformation. Deepfakes are increasingly being used to commit cybercrime – whether for financial gain, social disruption, voting fraud, or other nefarious purposes. In fact, the number of deepfakes identified online has skyrocketed from under 8,000 in 2018 to nearly 50,000 by 2020, and the latest estimate for 2023 is 500,000 (source: ResearchGate, Galgotias University, DeepMedia)(Exhibit 5).

Exhibit 5: Number of deepfakes identified online

Number of deepfakes increased 5x between December 2018 and June 2020



Source: Patel, M.M., Gupta, A., Tanwar, S., & Obaidat, M.S. (2020). Trans-DF: A Transfer Learning-based end-to-end Deepfake Detector. 2020 IEEE 5th International Conference on Computing Communication and Automation (ICCCA), 796-801. ResearchGate.

Cyber solutions

Luckily spending on cyber solutions is forecast to increase to a cumulative total of \$1.75 trillion by 2025, according to BofA Global Research. Areas of fast growth are anticipated to be AI, Zero Trust (a security framework that requires all users to be authenticated, authorized and continuously validated for security configurations before being granted access to applications and data), and Privilege/Identity Access Management, among others.

For all its challenges, AI is an important solution to the digital insecurities it creates. Extensive security AI and automation use have delivered cost savings of nearly \$1.8 million. Organizations with extensive use of security AI and automation demonstrated the highest cost savings comparatively, with an average cost of a data breach at \$3.6 million, which was \$1.76 million less and a 39.3% difference compared to no use. Even organizations with limited use of security AI and automation measured the average cost of a data breach of \$4.04 million, which was \$1.32 million less, or a 28.1% difference, compared to no use. However, organizations with no use of security AI and automation experienced an average cost of a data breach of \$5.36 million, which is 18.6% more than the 2023 average cost of \$4.45 million. Beyond the cost, AI can also reduce the time to identify a cyberattack by 100 days, help detect fraud & identify misinformation.

On that note, anti-fraud detection, identity verification and digital protection solutions should also be areas of focus. More than ever, consumers are transacting online, a trend that was further accelerated by COVID lockdowns. At the same time, eCommerce firms incurred ~\$20 billion in losses due to online fraud in 2021 and spent ~3x as much trying to protect themselves. As a result, the global total addressable market for fraud solutions is worth \$18 billion today and expected to compound at a 10-12% rate, according to TransUnion.

Cyber insurance

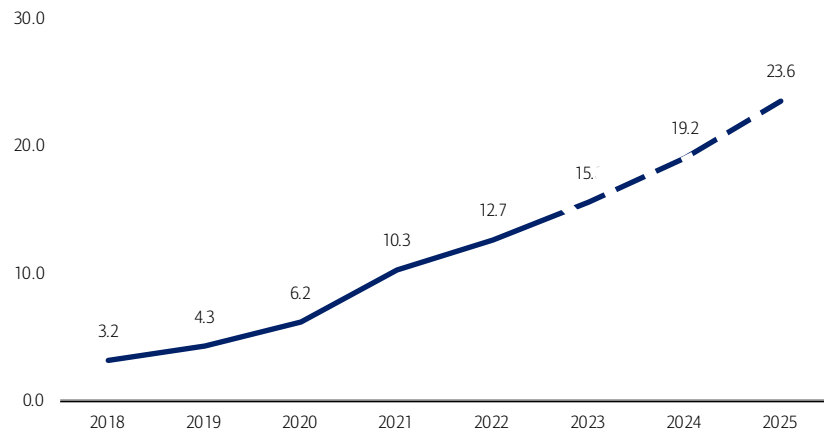
Cyber insurance, which first became available in the early 1990s, has historically been purchased to protect companies from the aftershock of data breaches, with typical policies covering data recovery, business continuity and liability risks of data privacy. However, as business models moved to the internet and later to the cloud, attacks began to evolve. Breaches became more expensive; data restoration became more complex; and data privacy regulations became stricter, which served as a catalyst for cyber criminals to raise ransoms.

As a result, there may be a growing role for cyber insurance following financial losses from data breaches and the rising number of hacks. And because of this, demand for cyber insurance should see market premiums rise to more than \$33 billion by ~2027 (from \$12 billion in 2022).

It's also important to note that first-order cyber insurance losses are close to \$1 trillion annually, but the market for cyber insurance supply covers only around \$6 billion, which implies a substantial coverage gap. The cyber insurance market grew ~25% in 2021, to \$10.3 billion, representing ~1% of total commercial insurance spend. The market is poised to grow at a 25% CAGR (compound annual growth rate) through 2025, reaching a total market size of \$23.6 versus the 9.7% CAGR of the broader commercial insurance market (Exhibit 6).

Exhibit 6: Cyber insurance market growth 2018-25 (\$bn)

The cyber insurance market is growing at a 25% CAGR through 2025



Source: MarketsandMarkets

Help wanted

Finally, it's not just about injecting more financial capital into cybersecurity, but also human capital. There is an industry-wide skills gap, with many organizations struggling to fill positions on their security teams. Some 10% of cyber leaders have indicated that they lack the critical people and skills needed to deal with a cyberattack (source: WEF). According to security leaders, 52% of jobs in their workforce require university degrees for entry-level positions (source: Information Systems Audit and Control Association (ISACA)), with one in five noting that it takes more than six months to find qualified cybersecurity candidates for open positions.

According to Cybersecurity Ventures, the number of unfilled cybersecurity jobs worldwide increased 350% between 2013 and 2021, from 1 million to 3.5 million. WEF estimates that there was a shortage of 2.27 million in 2021 and Fortune Magazine notes that more than 700,000 cybersecurity workers are needed to fill positions in the US alone. In fact, the number of open jobs in this field is enough to fill ~50 NFL stadiums.

There is also a gap from a gender perspective: women held 25% of cybersecurity jobs globally in 2022, up from 20% in 2019 and around 10% in 2013 (source: Cybersecurity Ventures). However, women held only 17% of Chief Information Security Officer (CISO) roles at Fortune 500 companies i.e., 85 out of 500 available positions.

Upskilling people to enter the cybersecurity workforce, especially women, would help address this issue, and initiatives could target soft skills, cloud computing knowledge and security controls experience.

But it's not just tech – physical security is also on the line

It's not just digital security people crave; people also want personal security (amid perceptions of rising crime), environmental safety (climate change) and good health (following the pandemic). But perceived "security" is easier said than done.

Consider this: Every 24 seconds someone is killed in a road traffic incident; that's 1.35 million people a year and projected to almost double by 2030. Meanwhile a 'silent pandemic' of antimicrobial resistance (superbugs evading antibiotics) could cause economic damage on par with the global financial crisis by 2050. And with 2023 not even over, the US has already set a record for the most climate-related disasters in a single year that cost \$1 billion or more.

Since the start of the 21st century, organized crime has killed as many people as all armed conflicts across the world combined. In the US, one home fire is reported every 93 seconds; one home fire-related injury occurs every 47 minutes; and one home fire-related death occurs every 3 hours and 8 minutes (source: NFPA). Also, an estimated 2.3 million people die from poor workplace safety every year with lost workdays costing the global economy ~\$3 trillion or almost 4% of world GDP.

But in getting back to basics, the words "safety" and "security" are often used interchangeably but have quite different meanings. Both are necessary for our survival, but in subtly different ways. Safety is the state of being protected against harm or danger, while security is the actions taken to make people or places safe. Safety is emotional or internal, while security is considered external or physical in nature (source: Kigs & Bamham). Overall, safety needs represent the second tier in Maslow's hierarchy (Exhibit 7) – and include security of body, employment, resources, morality of family, and health.

Exhibit 7: Maslow's Hierarchy of Needs

Safety needs represent the second tier in Maslow's hierarchy



Source: Maslow; Simply Psychology

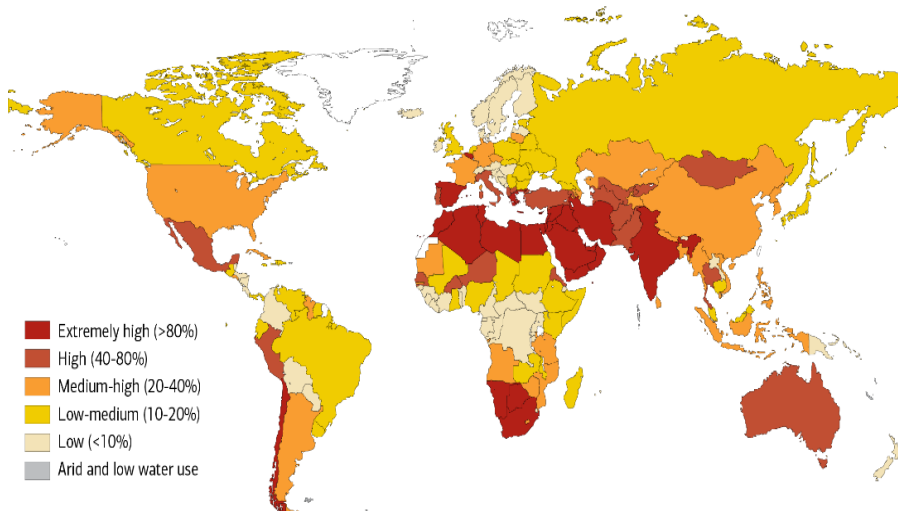
H2O no!

As mentioned in, [Global water scarcity: H2O no!](#), some 75% of our planet is covered with water, but less than 1% is usable, and even this is depleting quickly. Why? Water demand is up approximately 40% over the past 40 years and is estimated to increase another 25% by 2050, yet supply has more than halved since 1970. Today, around half of the world's population already endures extremely high water stress at least one month of the year, and at the current rate, we could run out of freshwater as soon as 2040. Additionally, as water scarcity worsens, \$70 trillion of global GDP (31%) could be exposed to high water stress by 2050, up from \$15 trillion (24%) in 2010.

WEF's Global Risks Perception Survey 2022-23 put natural resource crises within the top 10 risks in the next two and 10 years, and water certainly falls under this category. Through indirect channels, water has relevance to all the other top risks for both the two-year and 10-year time horizon with cybercrime and cyber insecurity (e.g., impact on water infrastructure), and large-scale involuntary migration as examples. In a similar vein, water has an impact on many other areas such as energy, food, biodiversity, and migration.

Exhibit 8: Average water stress by region, 2050

By 2050, an additional 1 billion people are expected to live with extremely high water stress



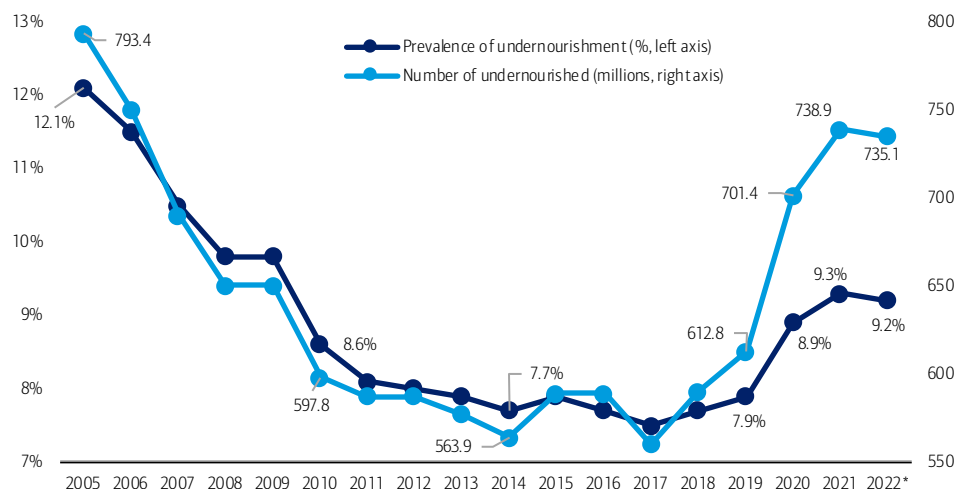
Source: World Resources Institute (WRI); Aqeduct

Food (in)security

Global hunger, measured by the prevalence of undernourishment, is still far above pre-COVID levels, affecting around 9.2% of the world population in 2022 compared with 7.9% in 2019 (source: UN) (Exhibit 9). In [Food \(in\)security: Hungry for Change](#), we note that the Food & Agriculture Organization of the United Nations (FAO) estimates that the pandemic increased incidence of hunger and lack of access to adequate food by over 300 million people from 2019 to 2020 alone. It is estimated that between 691-783 million people faced hunger in 2022 (source: WHO). And looking ahead, it is projected that almost 600 million people will be chronically undernourished in 2030 (source: FAO), pointing to the immense challenge of achieving the SDG (Sustainable Development Goal) target to eradicate hunger.

However, this issue is not evenly dispersed. When the price of food is raised, it largely hits lower-income countries the hardest and can lead to lower food security, acute shortages and, ultimately, social unrest. Wide-ranging solutions are needed, from increasing consumer education about healthy foods to making healthy foods more affordable and accessible.

Exhibit 9: The proportion of the world population facing chronic hunger in 2022 was about 9.2 percent, compared with 7.9 percent in 2019
Global hunger remained virtually unchanged from 2021 to 2022, but is still far above pre-COVID 19 pandemic levels



Source: FAO 2023. FAOSTAT: Suite of Food Security Indicators. NOTE: *Projections based on nowcasts for 2022.

Physical security solutions

Demand for public and enterprise safety solutions is rising against the backdrop of rising crime rates, natural disasters, etc. The total addressable market for this space grew from \$13 billion in 2016 to \$50 billion in 2021 and is expected to grow to \$60 billion by the end of 2023, implying a ~24% CAGR between 2016 and 2023 (source: Motorola Solutions). From a land mobile radio system (LMRS) perspective (a person-to-person, terrestrially based voice communication system), it is a \$12 billion TAM (total addressable market), consisting of infrastructure, devices (two-way radio and broadband) and software that enables communications. Video provides the largest portion of the overall TAM at \$22 billion, derived from cameras (fixed, body-worn, in-vehicle), access control, infrastructure, video management, software, and AI-enabled analytics. The command center software TAM is sized up at \$13 billion, involving software that enables collaboration and shares information throughout the public safety workflow from the initial 911 call to case closure. Lastly, managed & support services contribute a \$13 billion TAM, mostly related to LMR services.

Regular maintenance of fire and life safety protection systems is increasing the demand for building safety. In 2022, there were more than 116,000 commercial building fires in the US, resulting in over 1,000 injuries and more than 100 deaths. Fires in buildings with sprinkler systems have a 90% lower death rate versus fires in those without. However, regular maintenance is necessary to ensure fire & life safety are working properly. In 8% of US commercial building fires, sprinkler systems failed to operate. The most common reason was lack of maintenance preventing water from reaching the sprinklers. Other key fire and life safety equipment within buildings include fire alarms, extinguishers, panels, control panels, sensors, sprinklers and security and access control systems. The global fire protection systems market was ~\$83.8 billion in 2022 and is expected to grow at a CAGR of 8.6% to reach \$190.3 billion by ~2032 (source: Precedence Research).

Testing inspection and certification (TIC) along with security scanning equipment should also see growth in demand. For scanning equipment, impacted areas include aviation, ports, prisons, offices and shopping malls. These segments are highly regulated and are typically driven by government award cycles. Product certification and highly regulated markets create significant barriers to entry. TIC solutions are increasingly in demand over rising concerns around health, environmental, safety and security risks bringing regulatory complexities and conduct requirements, alongside higher quality, social accountability, and performance standards.

We need energy to heat homes and offices, cook food and provide power (see: [Utility bills](#) for more). There are two elements to ensuring safety of the supply chain. The first relates to logistics: obtaining source components, raw materials, and even finished goods. This can be influenced by temporary shutdowns of manufacturing resulting in cascading shortages along with personnel shortages affecting the distribution of labor.

The second supply chain safety issue relates to cybersecurity, specifically the ability to place complete trust in any product or solution's source code, firmware, system-on-chip, and other hackable parts. The challenge now is to ensure that the code and subcomponents of any solution are transparent and traceable so that the end client can be certain that the device, software, or

answer they receive is what they expected. As a result, the supply chain assurance security megatrend of 2022 was a hybrid trend combining logistics and cybersecurity. The industry is paying closer attention to this than ever before.

Physical and psychological safety in the workplace should also be a priority. According to Gallup, just 65% of workers are completely satisfied with their physical safety at work. That’s the lowest score in at least the last decade, following a high of nearly 80% in 2017. And it’s not just about physical safety but also psychological safety and mental health. Creating a safe and inclusive work environment is vital for fundamental employee well-being and productivity. A study showed that when employees feel psychologically safe, they exhibit 76% more engagement, 50% more productivity, 75% less stress and 30% more life satisfaction (source: Ecsell Institute).

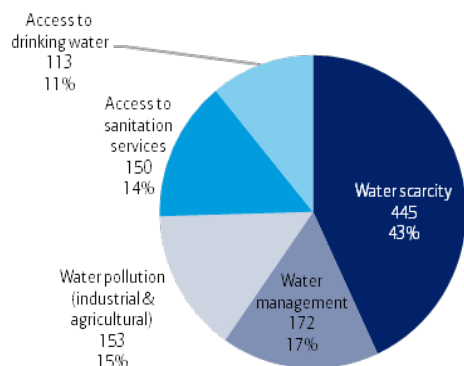
Water links in with nearly every other crisis we face. But did you know that every dollar invested in water access and sanitation could potentially generate ~\$7 in returns? The good news is it would cost only 1% of GDP annually until 2030 to solve the global water crisis. World Resources Institute (WRI) found that 75 countries can achieve sustainable water management at 2% or less of their annual GDP e.g., US and South Africa; 70 can achieve it with 2-8% of GDP; and 17 will require more than 8%. Water scarcity is the overall cost driver globally (Exhibit 10) but at a regional level, the estimated costs of addressing water scarcity are largest in North America and in East Asia and the Pacific (Exhibit 11). Sub-Saharan Africa and Latin America and the Caribbean have relatively lower water scarcity estimated costs.

An investment in infrastructure could be one of the first lines of defense against the water crisis. The implementation of water management and tech like smart meters, AI and smart irrigation could also result in better water use. Additionally, treatment like desalination is key for securing supply and already accounts for 90% of drinking water in some countries.

However, countries have different freshwater resources, population pressures, and water sector structures – privatized vs. nationalized etc. – which means that there is no one-size-fits-all solution to address the world’s issues. Instead, a combination of solutions is needed to solve the water problem: technology, investment, government regulation/policy, corporates and individuals managing water demand. See [Global water scarcity: H2O no!](#) for more on this topic.

Exhibit 10: Global breakdown of annual estimated costs for a sustainable water future until 2030 (2015 US\$ bn)

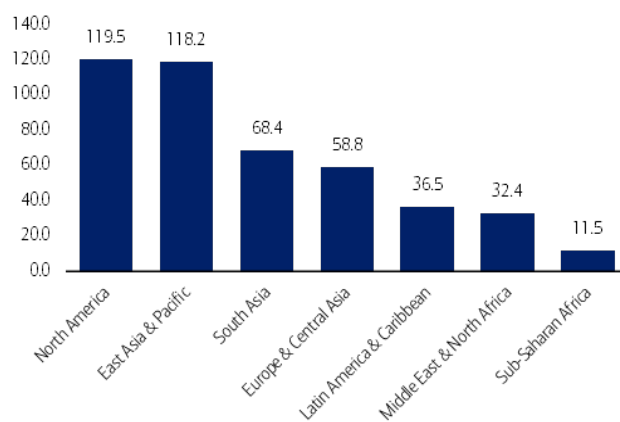
Water scarcity is the largest component (43%) of global costs



Source: WRI

Exhibit 11: Annual estimated cost until 2030 required to address water scarcity (2015 US\$ bn)

The estimated costs to address water scarcity annually are the largest in North America and in East Asia and the Pacific



Source: WRI, BofA Global Research

Global food consumption habits contribute to worsening climate and environmental crises while facilitating a wider public health crisis. Because of that, a range of near-term policy recommendations have been floated by a host of international agencies. Many of these recommendations fall into one of three broad categories: 1) education and communications, 2) affordability and accessibility, and 3) policies that link dietary needs with sustainability issues and national health guidelines. Ultimately, policy measures need to incorporate the interests of all stakeholders, from farmers and food producers to retailers and consumers. Policies need to be coordinated to maximize benefits while limiting negative trade-offs. Stakeholder responses should be measured and evaluated to enhance transparency and effectiveness. See [Food \(in\)security: Hungry for Change](#) for more on this topic.

Let technology step in with AgTech solutions. As discussed in our recent publication, [Feeding the future: How climate and agriculture intersect](#), the impact of climate change is multifaceted. The UN warns that climate change is set to expose up to 80 million more people worldwide to hunger by 2050. In fact, the global population, which is expected to grow by an additional ~2 billion people by 2050, will require the global agriculture industry to produce more food in the next 3-4 decades than was produced in the last 8,000 years (source: World Wildlife Foundation).

Innovations in AgTech can help to address environmental sustainability, food security, food safety, and farmworker health & safety by increasing efficiency and reducing input costs. The global AgTech market is expected to double to \$40 billion by 2030, which includes bioengineering, precision agriculture and genetic modification. Target areas for sustainability in agriculture include seeds, pesticides, bacteria-based pesticides and products, and new cover crops.

Biosecurity is also a growing concern as we enter a post-pandemic world with more infectious diseases. Pests are insects or small animals that can be harmful to humans and recent trends are contributing to an increased need for pest control. For example, more Americans are migrating south which is the only US region with positive domestic migration in 2022. In fact, almost half of the population growth in the US since 1960 has come from the South, supported by inward migration and a relatively high birth rate (see [Southern comforts](#) for more).

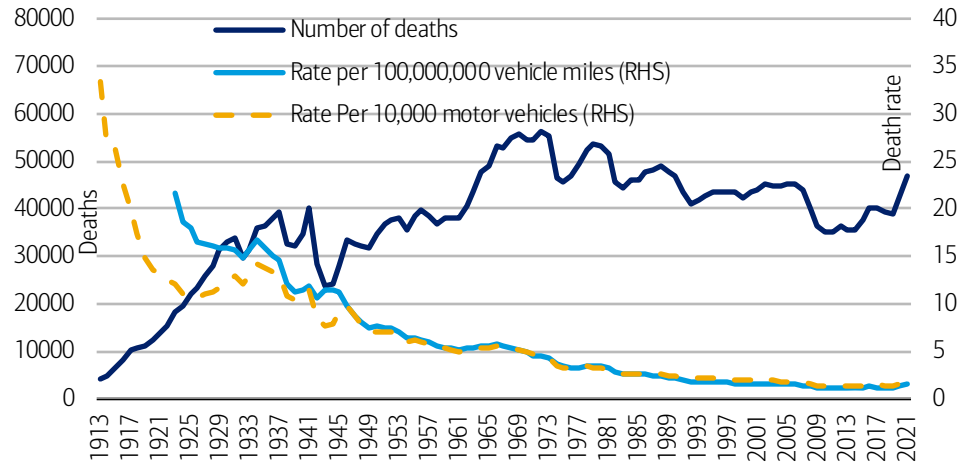
However, the warmer weather creates 3x the demand for pest control in the South compared to the national average. As pests prefer warm areas, climate change is another factor that has increased their harmful effects and the prevalence of pest-driven diseases and plagues. In warmer temperatures, insects reproduce faster, grow larger, and have higher survival rates in winter months. Pest control solutions include removing or destroying nests, blocking holes, temperature control methods, and traps to catch them and remove them from the area.

Issues behind the wheel

Transportation remains one of the most dangerous activities in our day to day lives. Road traffic accidents kill over 3,000 people per day globally – or someone every 24 seconds – amounting to 1.35 million deaths per year, not to mention the 50 million injuries that occur. In fact, road deaths are the number one killer of those aged 5-29 and the eighth highest cause of death for people of all ages, globally.

While overall road deaths per vehicle/mile have declined over time, they’ve begun steadily rising again since 2014. The death rate per 100 million miles driven in the US was 1.5 in 2021 vs. 1.14 in 2014, bringing decades of declines up to that point to an end. Many of those reductions were achieved through technological advances and the mandatory equipping of passive safety measures, such as seatbelts, airbags and crumple zones, which are now commonplace across all modern vehicles. But with 94% of road traffic accidents still attributable to human error (source: Own Rick and Solvency Assessment (ORSA)), it is hoped a combination of disruptive technologies can enable the next revolution in road safety improvements.

Exhibit 12: Death rates per mile/vehicle on US roads reached their lowest in 2011, but have since crept up again
 Dangerous driving: ~47,000 deaths on US roads in 2021



Source: US National Safety Council 2023; Number of Deaths and death rates per 100m miles and 10,000 motor vehicles in the US

On the road (to safety and solutions)

From accidents to automation: the shift in the global automotive market towards more automated driving features is driven primarily by safety. A new wave of active safety innovations in the form of Advanced Driver Assistance Safety (ADAS) systems are being deployed across transportation as the functionality improves and cost of development reduces with volume and exponentially increasing computational capabilities.

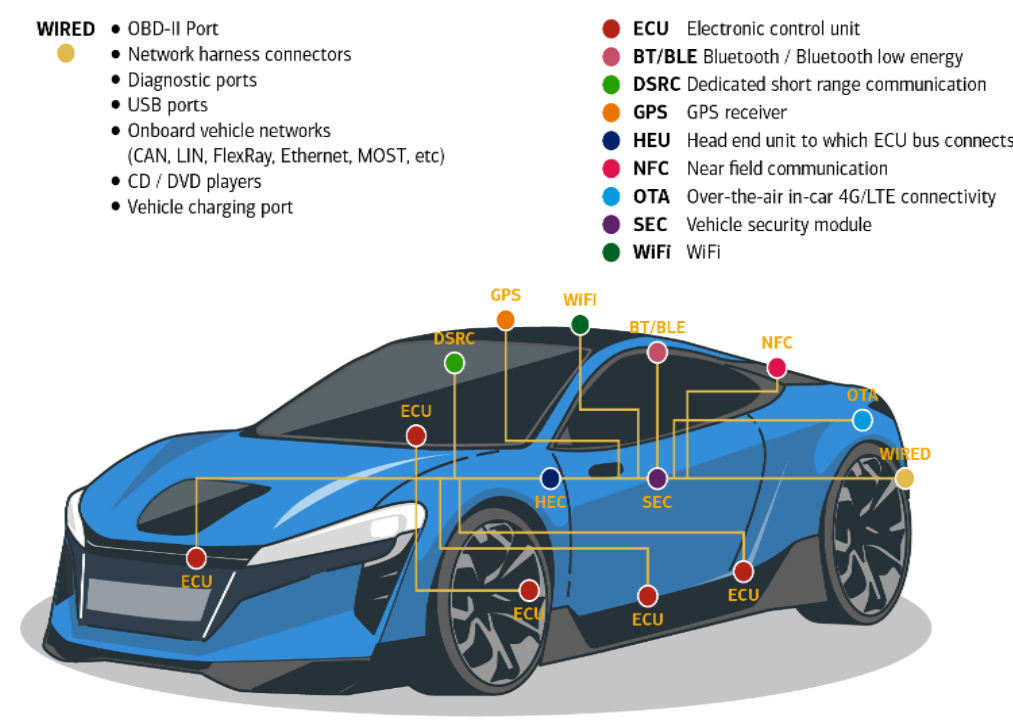
The US National Safety Council estimates these technologies have the potential to prevent >60% of road traffic deaths per year when deployed at scale, with a “sensor fusion” of radar, camera, ultrasound and lasers that gradually enable autonomous driving and safety interventions like emergency braking or collision avoidance. While more than half of cars didn’t have these technologies as of 2020, >90% penetration of the technology is anticipated by 2030. The global ADAS market is projected to grow at ~20% CAGR 2020-2025 to \$32 billion per BofA Global Research’s automotive research team.

Connected cars increase cybersecurity risk. As cars become more connected and autonomous, they are more at risk of cyberattacks, making automotive cyber solutions necessary. Today's cars already have up to 150 electronic control units (ECUs) and run on 100 million lines of software code, expected to rise to 300-500 million to enable increased safety and "software defined vehicle" features. To put this into perspective, a passenger aircraft has an estimated 15 million lines of code, a modern fighter jet about 25 million, and a mass-market PC operating system close to 40 million.

This increased code and expanding connectivity points dramatically raises the potential for cyberattacks, not only on the car itself but on all components of its ecosystem such as back-end infrastructure. To mitigate this threat, the auto cybersecurity market is projected to double in revenues between 2020-2030 to \$10 billion, with investments required in hardware, software and processes, per McKinsey.

Exhibit 13: Cybersecurity for the connected car

Even before cars become more highly automated, the threat level is increasing as digital and connectivity features are added



Source: Keysight Technologies, Microcontroller Tips

Addressing the swan (or rhino) in the room

















But what about unpredictable insecurity? COVID has taught us not to discount "black swans," which are unforeseen but high-impact risk events such as extreme weather disasters, mega earthquakes, super volcanos, asteroids, etc. Meanwhile, "grey rhinos" are probable events with high impact in contrast to the unpredictable nature of black swans. These risks are out there in the distance, but we don't clearly perceive their full dimensions. And finally, "grey swans" are events where we are aware of their possibility but equally understand that they are unlikely. However, if they do occur, the impact will often be highly significant.

So, in this world of unpredictable insecurity, black swans are increasing in frequency and impact; the average number of annual natural catastrophes has risen from 48 to 188 over the past 50 years. As we round out 2023, the US has set a record for the most natural disasters in a single year that have cost \$1 billion or more. There have been 23 extreme weather events in the US that have cost at least \$1 billion up until August 2023, which surpasses the record of 22 set in 2020. Last year (2022) was also deadly in that the 18 events of that year caused at least 474 direct or indirect fatalities – the 8th most disaster-related fatalities for the contiguous US since 1980. The costliest of these were Hurricane Ian (\$112.9 billion) and the Western and Central Drought / Heat Wave (\$22.1 billion), according to the National Oceanic Atmospheric Administration (NOAA).

And while black swans may be rare, we can't dismiss them outright. In fact, we are 10,000 years overdue a super volcano eruption that could disrupt global air travel and adversely impact agricultural harvests induced by global cooling effects. We are 150 years overdue a solar flare on the scale of the "Carrington event" that could cause mass global blackouts. There is a 99% chance of a major earthquake along the San Andreas fault line in California over the next 30 years. And every year wildfires around the world burn a land area larger than the size of India, while in the US wildfires burn down the equivalent land mass of New Jersey. The fact is: any black swan event would cost trillions of dollars and wreak havoc on the global economy.

Exhibit 14: What are Black Swans and Grey Rhinos?

Grey swans/rhinos include extreme weather/climate change, superbug resistance, whilst blackswans include solar flares, mega earthquakes, super volcano eruptions

Type	Characteristics	Example	Description
 <p>Grey Swans / Rhinos</p>	<p>Known unknowns (Unlikely, major Impact)</p>	<p>Extreme Weather</p> 	<p>Extreme weather events have increased significantly and this is likely to continue with global warming and climate change worsening every year. As the weather becomes more extreme, food, water, energy and flooding risks increase.</p>
		<p>Cybergeddon</p> 	<p>Cybergeddon refers to a large-scale hack of all computer networks and systems worldwide that would severely cripple the global economy because of our dependence on technology. It is essentially the digital version of the COVID pandemic</p>
		<p>Superbug Resistance</p> 	<p>Superbugs are strains of bacteria found to be resistant to some types of antibiotics. Antibiotic-resistant bacteria infect at least 2.8mn Americans each year and kill at least 35,000 of them. Antibiotics are used to treat the most common bacterial infections and higher resistance to them is often dubbed the 'silent pandemic'.</p>
		<p>Wildfires</p> 	<p>The risk of wildfires increases in dry conditions e.g. drought, heat waves. And as the weather becomes more extreme, the risk of wildfires increases. 2023 was the warmest summer on record and global warming is set to exacerbate wildfires.</p>
		<p>Job Automation</p> 	<p>The rise of Generative AI/ChatGPT brings a new dimensional threat to job security particularly for white collar workers. Job automation could increase inequality, breakdown of the social contract and economic disruption.</p>
		<p>Privacy Surveillance</p> 	<p>Are we heading into the Big Brother world of 1984? As privacy is eroded by surveillance technology and connected IoT world we could be heading into a future where more personal data is exposed.</p>
		<p>Inequality</p> 	<p>It's not just income inequality but also intergenerational inequality. Further divergence could cause more social unrest and instability.</p>
 <p>Black Swans</p>	<p>Unknown unknowns (Extremely rare, massive Impact)</p>	<p>Bioweapons</p> 	<p>Bioterrorism refers to the intentional release of biological agents or toxins for the purpose of harming or killing humans, animals or plants. The next pandemic could be bio-engineered in someone's garage using cheap and widely available technology such as CRISPR-Cas9</p>
		<p>Solar Flares</p> 	<p>A solar storm is a significant release of plasma from the Sun that would that disturbs the Earth's magnetosphere. Space weather events like these have been associated with negative tech damage such as blocked radio communications, satellite malfunction and disruption to rail networks and wireless networks, GPS. The most consequential effect though is extensive damage to transformers and therefore potentially long-term disruption to the electric power grid.</p>
		<p>Mega Earthquakes</p> 	<p>Neither the US Geological Survey nor any other scientists have ever predicted a major earthquake. Large mega thrust earthquakes that occurs in a subduction zone, where one region of the earth's tectonic plates submerge under another are estimated to occur once every 10,000 years on the US West Coast. Furthermore, Tokyo in Japan is also at high risk.</p>
		<p>Mega Volcanic Eruption</p> 	<p>We are 10,000 years overdue a super volcano eruption which are events in which at least 400 km³ of bulk material is expelled. High risk areas include Yellowstone, Mt Rainier in the US. Further, the eruption of the Toba super volcano around 74,000 years ago caused a global cooling of 3-5°C for several years and led to devastating loss of plant and animal life.</p>
		<p>Asteroid Impact</p> 	<p>The largest near-Earth asteroids could cause geologic and climate effects on a global scale and disrupt human civilization. Asteroids with >1km diameter have impacted Earth on average once every 500,000 years.</p>
		<p>Aliens</p> 	<p>NASA have probed hundreds of UFO sightings but found there was no evidence of aliens but the space agency also could not rule out that possibility. The odds of being the only technologically advanced civilization are 1 in 60 billion for the Milky Way.</p>
		<p>AI Singularity</p> 	<p>The growth of AI could be so uncontrolled and exponential that it results in machines overtaking humans.</p>

Source: BofA Global Research

Contributors

Vanessa Cook

Content Strategist, Bank of America Institute

Sources

Felix Tran

Research Analyst, BofA Global Research

Haim Israel

Research Analyst, BofA Global Research

Martyn Briggs

Research Analyst, BofA Global Research

Lauren-Nicole Kung

Research Analyst, BofA Global Research

Disclosures

These materials have been prepared by Bank of America Institute and are provided to you for general information purposes only. To the extent these materials reference Bank of America data, such materials are not intended to be reflective or indicative of, and should not be relied upon as, the results of operations, financial conditions or performance of Bank of America. Bank of America Institute is a think tank dedicated to uncovering powerful insights that move business and society forward. Drawing on data and resources from across the bank and the world, the Institute delivers important, original perspectives on the economy, sustainability and global transformation. Unless otherwise specifically stated, any views or opinions expressed herein are solely those of Bank of America Institute and any individual authors listed, and are not the product of the BofA Global Research department or any other department of Bank of America Corporation or its affiliates and/or subsidiaries (collectively Bank of America). The views in these materials may differ from the views and opinions expressed by the BofA Global Research department or other departments or divisions of Bank of America. Information has been obtained from sources believed to be reliable, but Bank of America does not warrant its completeness or accuracy. Views and estimates constitute our judgment as of the date of these materials and are subject to change without notice. The views expressed herein should not be construed as individual investment advice for any particular client and are not intended as recommendations of particular securities, financial instruments, strategies or banking services for a particular client. This material does not constitute an offer or an invitation by or on behalf of Bank of America to any person to buy or sell any security or financial instrument or engage in any banking service. Nothing in these materials constitutes investment, legal, accounting or tax advice. Copyright 2023 Bank of America Corporation. All rights reserved.