GreymatterFinch

# PRIORITISING IT GOVERNANCE

## *MAINTAINING TRUST IN TECHNOLOGY*

FEBRUARY 2024

> *"Emerging as the most severe global risk anticipated over the next two years, foreign and domestic actors alike will leverage misinformation and disinformation to further widen societal and political divides."*
> *- World Economic Forum: The Global Risks Report 2024*

### DEAR JOHN

In 2024, the world is still recovering from the aftermath of the COVID-19 pandemic, ongoing conflict in Russia-Ukraine and Israel-Gaza, and other political strife and economic constraints. These global challenges, coupled with climate change, rapid technological advances and disruption caused by AI, are causing wariness and division among many. We are in a state of flux on all fronts, and governance systems are stretched beyond their limits. But are our prospects as grim as it sounds?

## OUTLOOK UNCERTAIN

According to the World Economic Forum's[1] (WEF) Global Risk Report 2024[2], misinformation and disinformation are the biggest risks we will face over the next two years. The Global Risks Report 2024 presents the findings of the Global Risks Perception Survey (GRPS), which captures insights from nearly 1 500 global experts.

Following on **misinformation and disinformation** at number one are:

2. Extreme weather events
3. Societal polarisation
4. Cyber insecurity
5. Interstate armed conflict
6. Lack of economic opportunity
7. Inflation
8. Involuntary migration
9. Economic downturn
10. Pollution

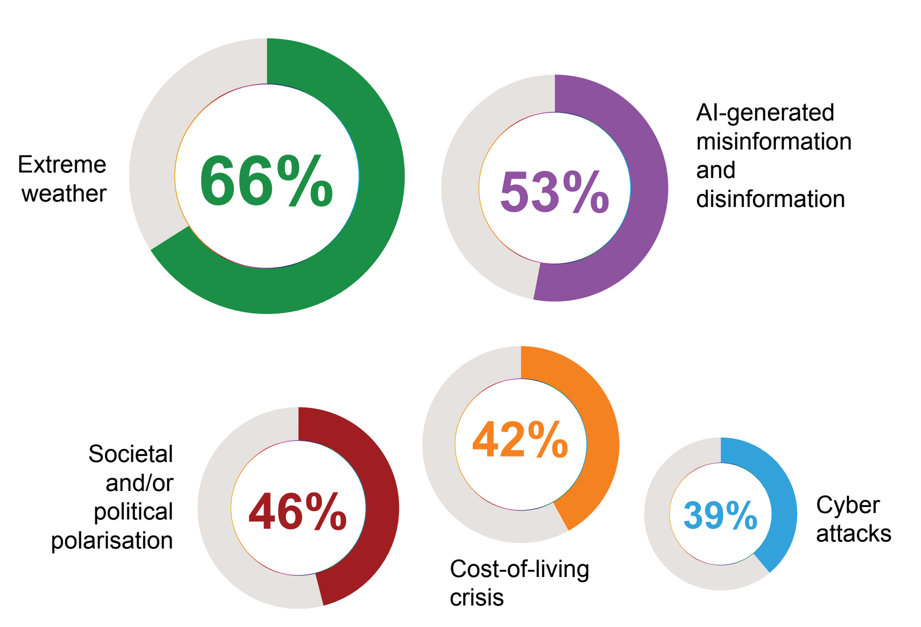
The long-term outlook over ten years puts climate change at the forefront:

1. Extreme weather events
2. Critical change to Earth systems
3. Biodiversity loss and ecosystem collapse
4. Natural resource shortages
5. **Misinformation and disinformation**
6. Adverse outcomes of AI technologies
7. Involuntary migration
8. Cyber insecurity
9. Societal polarisation
10. Pollution

As the short-term risks spread, they affect societal polarisation, the most extensively connected risk in the global network. Given the widespread mistrust in governments and news media, manipulated or synthetic content threatens to worsen existing conflicts significantly.

### CURRENT RISKS LANDSCAPE

When asked which five risks are most likely to present a material crisis on a global scale in 2024, the GPRS voted as follows:.




Close to three billion people in seven countries, including the United States, the United Kingdom, Russia and South Africa, are expected to head to electoral polls over the next two years. According to WEF, these risks could destabilise the legitimacy of newly elected governments, potentially leading to political unrest, violence and even terrorism. Technological advances, including generative AI, will enable the accessibility of information that could lead to the development of new tools of disruption and conflict, from malware to biological weapons. But they also warn that techno-pessimism is not helpful.

## HOW DO WE RESPOND?

As we advance as a species, our risks will increase. But so too is our capacity to respond. Extreme weather, AI-generated mis- and disinformation, a cost-of-living crisis, cyberattacks and socio-political polarisation are already upon us and are affecting billions of lives. The impact and timeline of each risk area are different, and so are our opportunities for mitigating or preparing for them. When combined, risks are heightened. But their worst outcomes are not inevitable. The solutions are already available. Today's crisis is an opportunity for a better future.

> *"We must recognise the full scale of the risk but maintain the optimism that we can and will respond in a way to avoid and mitigate the worst risks from occurring."*
> *- Gill Einhorn, Head, Innovation and Transformation, Centre for Nature and Climate, WEF*

Some challenges we face are risks familiar to human history, while others are new and fast-evolving. WEF reports that many global risks are interconnected and may have far-reaching consequences for human development.

But the future is not set in stone, says Saadia Zahidi, Managing Director of WEF. "A multiplicity of different futures is conceivable over the next decade. Although this drives uncertainty in the short term, it also allows room for hope."

Collaboration is essential for addressing global risks, but not all risks necessitate extensive global cooperation as the sole solution. In today's fragmented world, exploring different approaches that involve varying levels of cooperation can offer a more comprehensive framework for planning and preparation. The complexity and speed of global risks require adaptable and agile approaches that utilise all the tools at our disposal. We must take individual or collective actions to implement preparedness measures for unavoidable risks and collaborate to prevent or reduce the likelihood of avoidable ones.

According to WEF, there are four categories for approaching global risk reduction, based on the level of cooperation required:

**LOCALISED STRATEGIES**
Corporate and individual social responsibility and investment; collaboration between like-minded individuals and entities to promote local measures to present an agile response to risk.

**COLLECTIVE ACTIONS**
Good governance and responsible citizenship, changes in lifestyle or consumption patterns, and the independent effort of single citizens, companies and countries. If several people take such actions concurrently, such aggregate efforts have the power to alter market dynamics.

**BREAKTHROUGH ENDEAVOURS:**
Research and development.

**CROSS-BORDER COORDINATION**
Agreements on mutual restraint; addressing the weakest link in a system; international agreements on climate change; security maintenance and free trade.



## THE IMPORTANCE OF IT GOVERNANCE

The Global Network of Director Institutes[3] 2022-2023 Survey Report claimed that digital governance was an issue for boards of the future – not now. Digital transformation ranked fifth (only 21%) of priorities critical for organisational success, despite cyber-risk and digital innovation being identified by 55% and 54% of directors, respectively, as the two key areas that their boards have insufficient expertise/skills to govern over the next three to five years.

A well-known case study of continuous failure of IT governance that spans more than two decades is the case of the Post Office Limited (POL) Horizon IT scandal[4] in the United Kingdom. More than 700 sub-postmasters and postmistresses were prosecuted and convicted after faulty software made it look like money was missing from their branches. Some went to prison. Many were financially ruined. Some have died.

Records show that POL had more than 80 directors between 2000 and 2003. None of them probed or challenged the institution's narrative during this time. British Prime Minister Rishi Sunak has called it "one of the greatest miscarriages of justice in UK history" and has announced emergency laws[5] to exonerate and compensate victims.

Emerging technology governance faces a challenge known as the Collingridge dilemma[6], where early interventions are inexpensive, but the technology's full consequences are not clear, while later interventions are costly and complex once the need for change becomes evident.

### What governance lessons can be learned from this scandal?

1. The Board and its directors are responsible for IT governance. A complex governance structure can create **a lack of clear accountability** and cause confusion about who should oversee its governance.
2. Directors should not take arm's-length reports at face value and should have the **knowledge and experience** to interrogate the information supplied.
3. **An effective IT governance framework, policies and a robust IT-specific risk management strategy should be in place**. Boards must be vigilant in assessing and managing IT-related governance and risks, including cybersecurity threats, data breaches, and compliance issues.
4. **Regular IT audits and internal controls** are essential for evaluating the effectiveness and efficiency of IT operations. Boards should ensure these processes are in place.
5. **Large-scale procurement mistakes are difficult to unwind**. If supplier vetting and contracts are poorly managed, it is harder to hold suppliers to account.

In this context, the importance of effective IT governance has never been more pronounced. Effective IT governance plays an essential role in combatting the spread of misinformation and disinformation, which ranks as the foremost short-term risk in our increasingly digital world. The Collingridge dilemma, exemplified by past failures like the POL Horizon IT scandal, underscores the urgency of clear accountability, vigilant oversight, robust risk management, and regular audits in IT operations.

As technology's role in companies expands, IT governance is not a future concern but an imperative necessity for navigating the complexities of today and tomorrow, safeguarding against catastrophic failures, ensuring cybersecurity, and embracing the benefits of emerging technologies.

Sources: 1.https://www.weforum.org/; 2.https://www.weforum.org/publications/global-risks-report-2024/; 3. http://www.gndi.org/ 4.https://www.iod.com/; 5. https://www.bbc.com/; 6.https://www.sciencedirect.com/science/article/pii/S0048733317301622;

## READ OUR PREVIOUS NEWSLETTERS

[The biggest reporting milestones of 2023](#)
[How to be strategic about disclosure](#)
[The role of strategic design in reporting](#)