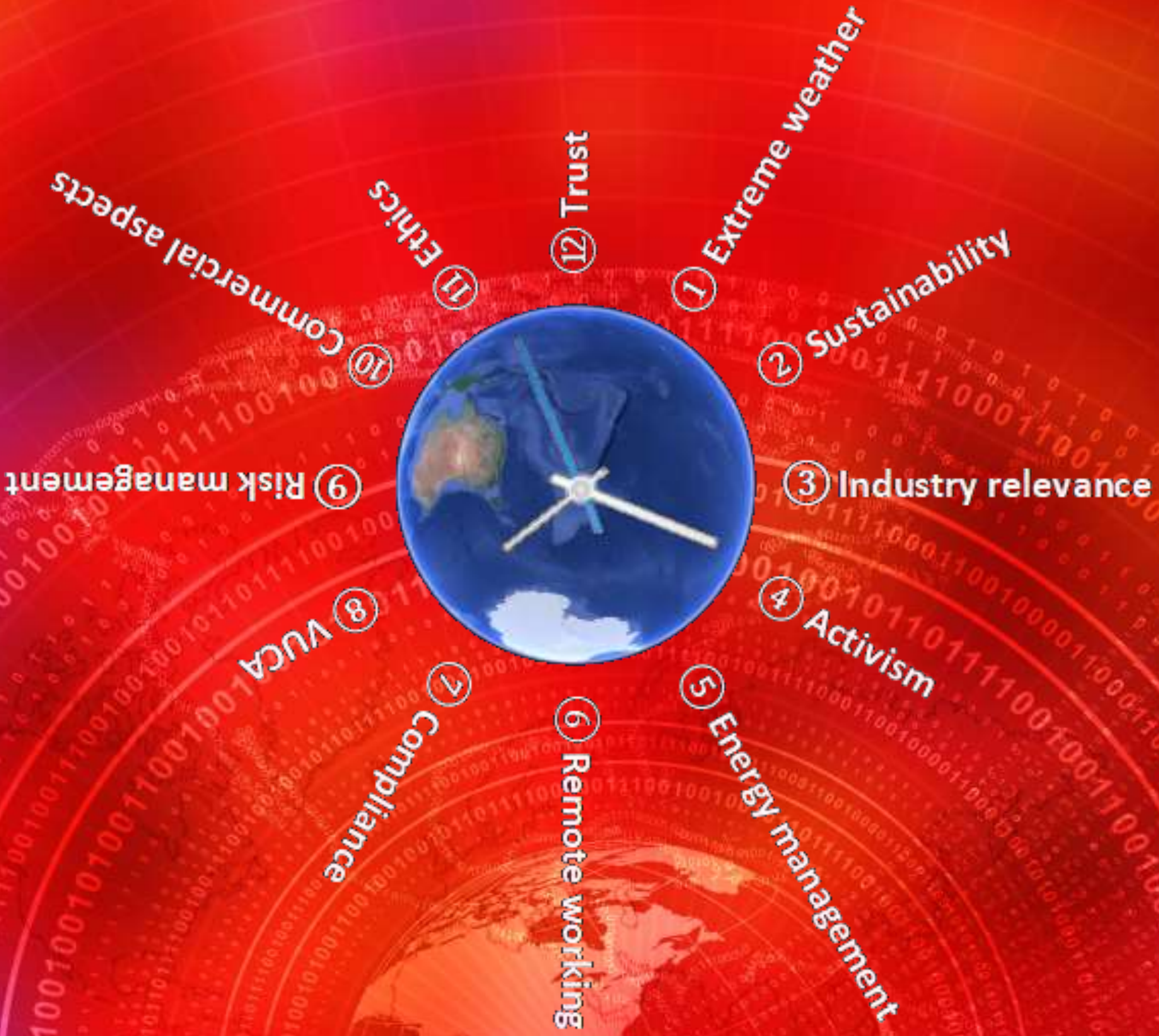
Secure the planet

The information risk and security profession takes on climate-change



Dr. Gary Hinson
January 2024

Contents

Summary

Climate change poses a raft of existential physical, business, safety and information risks, requiring proactive mitigation and adaptation strategies. Whereas you may think there is no common ground, this paper highlights a *dozen* areas of overlap between climate change and information risk and security management, presenting challenges and opportunities. It concludes with a call to action: six practical ways in which we can help.

Introduction

INTERNATIONAL STANDARD

ISO/IEC 27001

Third edition
2022-10

Information security, cybersecurity and privacy protection — Information security management systems — Requirements

Sécurité de l'information, cybersécurité et protection de la vie privée — Systèmes de management de la sécurité de l'information — Exigences

Reference number
ISO/IEC 27001:2022(E)

© ISO/IEC 2022

IN February 2024, ISO/IEC 27001:2022 was amended to incorporate "The Organization shall determine whether climate change is a relevant issue" (clause 4.1) and "NOTE: Relevant interested parties can have requirements related to climate change." (clause 4.2). So, one might well ask:

What has climate change to do
with information risk and security?
Is it relevant?

My purpose in publishing this paper is to broaden perspectives by pointing out a dozen links between the two fields, prompting information risk and security professionals to consider their positions, evaluate their options and initiate or promote the appropriate corporate responses.

We can *all* play our part in tackling climate change – including the information risk and security profession. No, really, we *must*, and soon. The clock is ticking. Snap out of your slumber before the alarm sounds!

A dozen points of contact

In response to those rhetorical questions in red above, 12 linkages between climate change and information risk and security are described below. Whereas most points constitute risks, there are also some genuine opportunities here for astute readers, hinting at the possibility of a *proactive* rather than purely *reactive* approach.

Reading each of these points only requires a minute or so. Thinking and talking through the implications in your specific context and deciding how to respond may take some hours.

① Extreme weather

The news headlines and statistics tell us that 'weather events' are increasing in both intensity and frequency. Although the root causes are not universally accepted as anthropogenic, even among scientists, climate change itself is clear from the environmental data. It is certainly happening.

"We have a problem, Heuston"

Increasing global temperatures are literally evaporating the oceans, leading to increasing rainfall, severe storms and flooding. At the same time, melting ice caps are raising sea levels, threatening coastal and low-lying areas, not least several major cities. Wildfires are adding to the intentional human destruction of native forests, the smoke and fumes exacerbating the greenhouse effect of water vapour, carbon dioxide, methane, burnt hydrocarbons and other atmospheric pollutants.

Serious and widespread incidents can have business – and life – continuity implications, in other words there are increasing risks of physical damage and business disruption. Aside from the direct impacts of local storms and floods, there are regional, national and even global effects, such as increasing insurance costs and stronger planning and building regulations.

Physical security is an integral part of information security. Aside from protecting computer systems against physical damage, ensuring the health and wellbeing of the workforce is crucial to protecting and exploiting the valuable intellectual property inside workers' heads.

② Sustainability

The way in which organisations respond to climate change is a hot topic in management circles. Although information about emissions, consumption of fossil fuel, environmental damage *etc*. is being widely gathered, analysed, used and published, the quality and integrity of this information is somewhat dubious, leading to claims of 'climate change denial', 'hidden agendas' and 'greenwashing' – a little cluster of information risks and possible incidents (*e.g.* when false claims about emissions reductions are revealed, scandalously).

There are genuine concerns about commercial exploitation and political manipulation in emissions trading schemes, for instance, along with dubious corporate announcements and disclosures concerning environmental performance.

Subjectivity and perspective are parts of the problem: a typical oil company executive, for example, has a rather different take on climate change than, say, a scientist researching coral bleaching. They each have some control over environmentally-relevant information, and latitude to express their own beliefs, understandings, prejudices and biases in the process (perhaps unintentionally and unknowingly).

The scientific approach itself complicates matters. The combination of complex theoretical models with finite experimental data usually leads to probabilistic rather than absolute conclusions, with confidence limits and *caveats* in scientific papers … that non-scientists may misinterpret as sinister rather than honest, factual disclosures.

Having said that, powerful vested interests implies the possibility of corruption and fraud. However, as time marches on, data accumulate and reasoned opinions strengthen, more extreme positions become untenable, leading eventually to 'corrections' or 'adjustments'.

Aside from *environmental* and *life* sustainability, there are *business* sustainability aspects noted throughout this paper.

③ Industry relevance

Some industry sectors are particularly affected by climate change - obvious examples being those closely associated with and (historically) heavily reliant upon fossil fuels (*e.g.* coal mining, oil exploration and refining, all forms of transportation, electricity generation, HVAC, chemical and plastics production, smelting, tourism ...), plus those involved in the response (*e.g.* governments, law enforcement and other emergency services, forestry, farming, fishing, research, electricity generation, transportation, healthcare ...).

Even industries with *beneficial* environmental impacts face risks resulting from climate change impacts on their supply networks (suppliers, partners, customers …), workforces and society at large. They also have enormous potential to find/create and exploit opportunities, with all the usual challenges relating to innovation, commercial naiveté, rapid expansion and intense competition.

There are various business and cyber risks here, hence corporate risk management should at least *consider* the potential ramifications, ongoing changes and strategic implications.

④ [H]activism

"The Earth Liberation Front, also known as 'Elves' or 'The Elves', is the collective name for autonomous individuals or covert cells who, according to the ELF Press Office, use 'economic sabotage and guerrilla warfare to stop the exploitation and destruction of the environment'." (Wikipedia). They are not unique.

Although environmental pressure groups have hitherto been quite benign and restrained, it is *possible* that we may see more overt and perhaps violent green activism, applying pressure to industries, organisations and governments that are alleged to have resisted and responded reluctantly, slowly and ineffectually to climate change. As the effects of climate change become ever more visible and undeniable, the fossil fuel industry in particular considers eco-terrorism (environmental extremism) a legitimate concern, a genuine security threat. Given the preceding point about industry relevance, other sectors (including the scientific research community) may also be targeted, while of course *all* sectors may be impacted if escalating actions cause serious, widespread and prolonged incidents.

These days, social and news media are powerful weapons for pressure groups to promote their interests, coordinate their activities, solicit support, lobby politicians *etc*., while hacking/hacktivism is one means of gathering and disseminating sensitive information about greenwashing, fraud and corruption. We are already seeing early examples of AI-powered misinformation and disinformation, social media campaigns, political lobbying and anti-democratic practices.

Conceivably, spies and spooks are already actively working to promote national interests, exploiting opportunities for political, economic, commercial and societal advancement relating to climate change (*e.g*. stealing intellectual property behind green electricity and electric vehicle technologies).

⑤ Energy management

Energy consumption is obviously relevant to computers and other electronic devices. Computationally-intensive AI systems are already in the media spotlight for their alleged eco-unfriendliness, along with general concerns about the megawatts supplied to and emitted by large data centres … all the way down to power consumption by individual pieces of IT equipment.

IT energy efficiency is an increasing concern, with implications for system performance optimisation, standby energy consumption *etc*.

The collection, analysis and use of information concerning energy supply, consumption, efficiency *etc*. is essentially digital data processing with various cyber risk and security implications. For example, power consumption by 'smart grid' IoT devices can be remotely measured and controlled to help stabilise national power grids, raising concerns about data, device and network security.

Renewable energy supplies such as wind generators and solar panels have various risks but, provided they are soundly engineered (well specified and designed, engineering, installed, tested, operated, managed and maintained), offer advantages in terms of grid independence, cheaper power and, of course, environmental benefits over traditional electricity supplies. Proper engineering of power systems includes their data monitoring, controls and security (*e.g.* ensuring the quality, integrity and availability of supply, and controlling access to the management functions) plus supply chain security for commercial systems.

At the deeper level of IT/OT hardware, CPU internals, firmware and software (including device drivers, operating system functions and utilities), power management is just one of many system functions subject to all the usual cyber threats, vulnerabilities and impacts. Except perhaps for those smart devices, the cyber risks are low … but not zero, hence in some contexts, spooky supply chain compromises (backdoors, kill switches), malware and hacks may be of concern, along with humdrum risks such as human error (flaws, bugs, insecure configuration …) and technical fallibility (component failure, performance degradation, unreliability …).

Energy monitoring and control increases the complexity of systems, a very generic and broadly-applicable information risk. To illustrate the point, can your UPS or facilities maintenance engineers and electrical contractors be trusted to work unattended, out of hours, inside the computer suite? Are they trustworthy, competent and careful? Should they be identity and background-checked, made aware of their information security obligations, signed in-and-out, accompanied and overseen by trusted insiders, monitored on CCTV *etc.*? Is their diagnostic equipment free of malware?

On the upside, a strategy of reducing power consumption through the replacement or retirement of older energy-efficient power-hungry systems is a plus for cyber security as well as the environment. Less power supplied equates to less heat to dispose of, reducing temperature stress and fire risks … provided any replacement systems are soundly engineered.

⑥ Remote working

Another festering cluster of information risks arises from the precipitous change to home-working for managers and professionals through COVID lockdowns. Global socio-economic changes were brought about by the pandemic, and we face lingering concerns as the world gradually adopts ‘a new normal’.

Commuting and other forms of transportation are environmentally costly activities, hence there is pressure to avoid or reduce unnecessary travel, begging questions about the necessity to travel. Climate change, then, is just one of several factors leading to a sustained increase in remote and mobile working, exploiting portable technologies and ubiquitous networking capabilities. The proliferation of laptops, smartphones, wearable IoT *things*, wireless Internet connectivity and *ad hoc* networking presents a raft of opportunities and, yes, cyber risks.

⑦ Compliance

Compliance with environmental laws, regulations and standards involves data/information with information risk, security, assurance and ethical implications. Remember dieselgate in 2015? …

> "The United States Environmental Protection Agency (EPA) discovered that certain VW diesel vehicles were emitting higher levels of nitrogen oxides (NOx) than allowed by law. NOx emissions contribute to air pollution and can have negative impacts on human health, particularly in urban areas where traffic is heavy. Upon further investigation, it was revealed that VW had installed software, known as a 'defeat device', in its diesel vehicles that would only activate the emission controls when the vehicles were being tested. During normal driving conditions, the emissions controls were turned off, allowing the vehicles to emit much higher levels of NOx than allowed by law." (Envirotech-Online).

Adding to the information integrity aspect noted above, there are confidentiality and availability requirements - in other words, information risk and security are relevant here. Environmental information deserves to be protected and (legitimately) exploited like any other.

The publication and promotion of corporate environmental sustainability policies or statements, for instance, is a commitment that should be backed by credible evidence of action and progress.

> "Cybersecurity is the second greatest threat to the globe, only after climate change."
>
> *Colton LeBlanc, Canadian Minister of Cyber Security and Digital Solutions*

⑧ VUCA

Taken as a whole, climate change contributes to VUCA (**V**olatility, **U**ncertainty, **C**omplexity and **A**mbiguity). At a very broad level, it presents awareness opportunities in the general area of risk management, including information risk and security management, assurance, compliance, resilience, continuity and so on.

Adopting good practices (or at least actively avoiding bad practices!) in relation to environmental sustainability is conceptually similar to other good practices such as the ISO/IEC 27000-series information security standards. Despite the uncertainties and practical limitations, there are valuable business, economic and social reasons for adopting a proactive, systematic approach, foreseeing, evaluating and responding appropriately to unpredictable future events.

Inaction or resistance, in contrast, is riskier and potentially far more costly - existential even.

⑨ Risk management

Climate change has implications for information risks such as those identified in the remainder of this paper, plus:

- Supply chain disruptions causing unreliability, shortages and increased costs for important products (goods and services) and resources *e.g.* water, energy, data centre and cloud computing services, AI, electronic components and ICT devices;
- Greater reliance on backups and a more limited choice of alternative, local sources (to reduce long-distance transportation), possibly of lower quality, higher costs and weaker security (more susceptible to malware, hacking, fraud and espionage, plus novel attacks and compromises);
- Breakdowns of social order, increasing civil unrest and disobedience resulting from food and water insecurity, shortages and inequality, inflation, mass migration to escape flood- or storm-prone areas *etc*. leading to an increase in crime levels including cybercrime, vandalism, violence, theft, looting, vigilantism and other incidents exploiting the over-stretched authorities.

Taking a truly dystopian view, governments seeking to protect critical infrastructures from marauding mobs enraged by widespread social and economic issues linked to global warming may be forced to resort to military intervention and control of facilities, commandeering resources and imposing Marshall law amid political, economic and social chaos. Is your organisation even *remotely* prepared to address the possibility of civil/national, regional or even global war? Who is responsible for tracking and tackling such extreme risks?

The risk component of climate change presents opportunities to raise management's awareness and appreciation of concepts and terms of art such as risk, threat, vulnerability, impact, response, continuity, resilience, recovery and contingency.

⑩ Commercial aspects

Clearly there are both costs and benefits to environmental sustainability. From an economic perspective, most of the costs are internal (paid by those installing solar panels *etc*.) involving investments in the near-term as we green-up, whereas most of the benefits are external (accrue to society) and delayed over decades.

What's worse, the benefits and costs are uncertain, making green investments inherently risky in purely financial terms. Once again, there are implications for the integrity and availability of the data, analysis and management decisions – yes, this is yet another information risk issue.

There may be opportunities to retire older energy-hungry ICT devices, replacing them with more energy-efficient and generally more secure modern equivalents, simultaneously reducing both the carbon footprint and the organisation's risk profile.

Naturally, we should ensure that old equipment and media are properly sanitised of any confidential data, either in-house or using a trustworthy contractor.

Conversely, corporate policies to reduce eWaste by retaining and utilising old equipment for longer should take account of the cyber risk implications, such as ensuring they remain fully supported by whoever is responsible for vulnerability management and patching.

⑪ Ethics

Organisational responsibilities extend *beyond* obvious stakeholders such as the workforce, owners/investors, customers and authorities. Environmental impacts are often diffuse and widespread. Ultimately, all life on Earth depends on the global biosphere, a shared, finite, irreplaceable and invaluable resource.

There is a tragedy of the commons here, in that those who delay or refuse to invest in environmental sustainability may reap the short-term cost savings *and* the long-term benefits of the concerted actions of their more responsible halo-sporting peers. On the other hand, they risk being caught in the act and pilloried by society, shunned by investors, excluded from lucrative contracts and perhaps penalised by the authorities. Furthermore, if/when they are eventually forced to up their game, they may find their options limited, suffering additional costs to catch-up rapidly with the rest of the world. Once again, there are risks here.

While terms such as ESG (**E**nvironmental, **S**ocial and **G**overnance) and CSR (**C**orporate **S**ocial **R**esponsibility) may be out of favour among MBAs, the concepts indicate management's recognition and acknowledgement of the expectations of, and corporate obligations towards, human society. Behaving ethically encompasses the idea of equality, mutual respect and fairness, with strong integrity implications … which makes it an information risk and security concern as much as a **H**uman **R**esources and general management matter.

⑫ Trust

Throughout this paper, I have raised various commercial/contractual and ethical concerns, including policies, accountability, responsibility, expectations and obligations. The concepts of trust, trustworthiness, mutuality, integrity, honesty, fairness and assurance form both a fundamental basis and a risk management framework.

To what extent can we believe various corporate statements and reports on environmental performance and aims? What can we do to ensure our own organisation's disclosures are believed? The answer involves a combination of factors such as: the veracity of the information and the way it is presented; the quality, breadth and depth of data on which the disclosures are based; and the organisation's track record as a trustworthy and honest business. That final point cuts both ways: genuine and reliable environmental disclosures, supported by sound data and robust analysis, can strengthen the corporate brand, and *vice versa*. In other words, they are, in part, marketing information with integrity implications.

"Greenwashing presents a significant obstacle to tackling climate change. By misleading the public to believe that a company or other entity is doing more to protect the environment than it is, greenwashing promotes false solutions to the climate crisis that distract from and delay concrete and credible action … The science is clear: greenhouse gas emissions, such as carbon and methane, from human activities are wrapping the Earth in a blanket of pollution that has warmed the planet and led to severe impacts such as more intense storms, droughts, floods and wildfires." (United Nations).

An eco-security action plan

1. **Assess your organisation's risks relating to climate change** *e.g.* by incorporating climate change scenarios into your regular risk management workshops and courses. Identify dependencies on critical national/corporate infrastructure. Consider cascading effects (such as supply chain disruption and civil unrest) and assess the business continuity implications of cybersecurity incidents caused by or arising from climate change.

   *[**Hinson tip**: rôle-play or red-team eco-terrorists picking fights with big industry to kick up a stink and force action.]*

2. Help management **build integrity in** to the organisation's environmental strategies, plans, policies and approaches including data analysis.

   *[**Hinson tip**: clarify and laser-focus on key objectives, including those at the intersection of information risk and sustainability …]*

3. Invest in **corporate resilience** for the ICT infrastructure and vital information services, plus supply chains, as a strategic objective. Engineer them to reduce dependence on vulnerable information sources, systems and organisations that deny, ignore or are reluctant to respond to climate change.

   *[**Hinson tip**: resilience is a general-purpose control with substantial business benefits for all manner of challenging circumstances and incidents. Think ahead and prepare. Dig the well before you get thirsty.]*

4. **Facilitate and encourage *secure* remote working** using appropriate technologies (*e.g.* cloud computing), cybersecurity controls (*e.g.* **M**ulti-**F**actor **A**uthentication, laptop encryption, **V**irtual **P**rivate **N**etworking and **M**obile **D**evice **M**anagement) plus policies, procedures, training and support (*e.g.* out-of-hours incident reporting and response), reducing the need for travel.

   *[**Hinson tip**: provided remote or hybrid working is viable, this is an opportunity for information risk and security to support the business and the workforce by tackling the security aspects proactively. Security should not be a barrier to remote working. You might even want to promote that position overtly within the company, increasing social/political pressure on other resistant parts of the organisation and individual managers to at least permit if not encourage remote working where appropriate.]*

5. **Raise awareness**. Integrate climate change-related risks and responses into your security awareness program for *all* workers, influencing the corporate culture. For example, raise the possibility of phishing and other social engineering attacks, misinformation *etc.* exploiting chaotic crises and concerns relating to storms, floods, fires and other climate-related incidents. Take advantage of workers' green interests by recruiting awareness champions to help disseminate and reinforce key security *and* sustainability messages.

   *[**Hinson tip**: squeeze double the value from the security awareness program by encouraging workers (including IT and cybersecurity professionals) to minimise their carbon footprints and climate change risks as well as their information risks, for instance minimising energy consumption by retiring inefficient ITC devices and making good use of built-in device power management and standby functions.]*

6. **Collaborate** with others including colleagues from IT/OT, Risk Management, Compliance, Internal Audit *etc.*, plus government agencies, energy providers, technology companies, plus industry peers and even the academic/research and voluntary sectors. We're all in this together, so share intelligence and disseminate good practices.

   *[**Hinson tip**: might this very paper be of interest to your risk and security colleagues/peers, social media contacts and special interest groups? Do us all a favour and pass it on - please.]*

By proactively integrating climate change considerations into information risk and security management strategies and approaches, we can build more resilient organizations, protect critical national and corporate infrastructures and mitigate the existential risks relating to this complex, evolving challenge.

Conclusion

Information risks are highly context-dependent, including those identified in this paper. Contrast, for instance, the concerns on a nuclear submarine with, say, a farm, a mature manufacturer versus a greenfield startup, a family-owned craft business serving the local community as opposed to a sprawling multinational with a diverse product portfolio. The threats, vulnerabilities and impacts all vary in relation to other risks and other management concerns/interests.

It is down to you to think through the implications, identify and assess your information risks, and (in conjunction with colleagues and management) treat them appropriately. On behalf of mankind and the global ecosphere, I entreat you to do your best. We're counting on you to seize this opportunity to make a difference, and help save the planet.

Further reading

- The **U**nited **N**ations is actively coordinating and promoting a global response to climate change: www.un.org/en/climatechange
- The **IPCC** (**I**ntergovernmental **P**anel on **C**limate **C**hange) is a UN body overseeing and promoting climate change science: www.ipcc.ch/
- ISO directive on climate change in the management systems standards: committee.iso.org/sites/jtcg/home/news/content-left-area/news-and-updates/deciphering-the-latest-changes-t.html
- IAF/ISO Joint Communiqué on the addition of Climate Change considerations to Management Systems Standards (February 2024)
- Explore ISO/IEC 27001 and other good practice standards at ISO.org and ISO27001security.com
- If you were at RSA 2023, maybe you caught Chloé Messdaghi's presentation "The elephant in the security room: climate change". If not: www.techtarget.com/searchsecurity/feature/Where-climate-change-and-cyber-attacks-intersect

About the author

With a PhD in molecular biology/microbial genetics (a *long* time ago!), I am a scientist through and through.

Despite having pivoted into IT and then information risk and security management nearly four decades ago, I retain a deep fascination with science, research, technology and data.

I am strongly rational by nature, yet self-aware enough to recognize my emotional attachment to environmental and humanistic issues. I passionately believe we need to protect Earth's fragile biosphere against further harm, *now*, before it is broken beyond repair.

Little voices in my head warn that it's too late already. "Life on Earth is doomed, Gary", they whisper. "We've sealed our own fate" … and yet I'm convinced we can at least slow our descent into the seething volcanic crater, and determined to play my part.

So, will you help?