



Shaping society 5.0 Building trust in AI as a force for good

How AI-powered risk management solutions can support cybersecurity and build trust



Foreword



**By Harold Pradal,
Chief Commercial Officer, BSI**

2023 will be viewed as the point that Artificial Intelligence (AI) tipped into the mainstream, with a 286% rise in media coverage of the topic¹. And whilst headlines were grabbed by ChatGPT, the real AI story is much, much deeper.

This transformational technology is accelerating progress – and has the potential to go further as a force for good and move us towards Society 5.0, a ‘human-centered society that balances economic and technological advancement to solve society’s problems’². Importantly, it also raises questions around how we build trust in AI and what guardrails are needed to ensure AI shapes our future in a positive way.

In this collection we go behind the headlines to explore the real-world impact of AI through the eyes of BSI experts, drawing on the views of 10,000 people in nine countries. For anyone in doubt, AI is here and it’s here to stay – 38% of people use AI in their jobs daily, rising to 70% in China and 64% in India. By 2030, 62% expect their industry will use AI³.

At BSI we are committed to shaping the impact of technology and innovation for the benefit of individuals, organizations and society. AI sits at the heart of this because it has the potential to be a powerful partner, changing lives and accelerating progress towards a better future and a sustainable world.

We commissioned these essays to turn the spotlight on this generational opportunity – recognizing that the better we understand it, the better we can harness its power. Whether it’s creating new workplace opportunities, improving patient outcomes, tackling modern slavery or building a safe global food system, AI has a pivotal role to play.

We examine the importance of embedding digital trust in AI, the critical role for collaboration – between nations, policymakers, organizations and individuals – to unlock AI’s true potential, and the fast-evolving regulation designed to ensure consistency and certainty.

With AI crossing over from small, contained environments into mainstream technology at work and at home, this offers a transformational opportunity to unlock a multitude of benefits – provided trust and confidence are present too.

AI is just getting started. At BSI we are excited to partner with our clients as we embark on this journey. We are delighted to present these essays to explore the enormous potential AI offers to shape Society 5.0 and deliver a sustainable future powered by innovation.

1. Signal search analysis 2022-2023.
2. Society 5.0: The Fundamental Concept Of A Human-Centered Society, Open Business Council, Aug 2023
3. BSI Trust in AI Poll 2023



How AI-powered risk management solutions can support cybersecurity and build trust

As a purpose-driven organization, BSI believes AI can be a force for good, changing lives, making a positive impact on society, and accelerating progress towards a sustainable world. In this essay, Mark Brown, Managing Director – Digital Trust Consulting, sets out how AI can be used to address cyber vulnerabilities, shape trust and partner with individuals and organizations on their digital journey.





By Mark Brown

Managing Director, Digital Trust Consulting, BSI

Journeys worth taking often carry an element of uncertainty – and the digital journey is no exception, throwing up a number of cybersecurity considerations around personal data and who has access to information. As AI accelerates the road to digital transformation and Society 5.0, shaping how we work, rest and play, it has the potential to be a force for good for those who are well prepared and focused on building digital trust.

You could be forgiven for thinking that AI was new on the scene, given the extent of global coverage of developments such as ChatGPT. Analysis using the Signal monitoring tool suggests coverage in top media titles of AI rose 286% in the first half of 2023 compared to the preceding six months¹. In fact, it's been revving up for years and has long been a regular discussion point at major global events such as the G7, G20 and the World Economic Forum (WEF), as shown by the latter's 2018 Future of Jobs report².

What's new is that AI is now crossing over from small, contained environments into mainstream technology at a consumer level, as McKinsey's research shows³. This brings added risk. Importantly, it offers added opportunity to drive progress across society – for those who know how to unlock it. AI has the potential to positively shape our future, including when it comes to making us more cyber-secure.

- With AI tipping into the mainstream, there are strong benefits that can come from educating the public to build trust.
- AI can function as a cybersecurity gatekeeper, but having the right 'risk appetite' can help organizations accelerate progress to building greater digital trust.
- Not all data sets are equal and recognizing this is key to unlocking their true potential.
- In the future, the ideal situation will be cybersecurity managed as a partnership between people and AI.

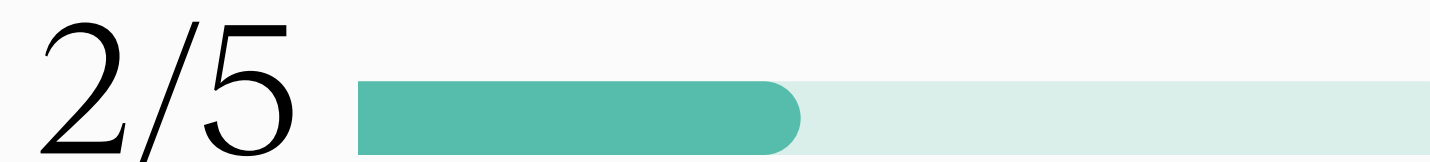
286%

Analysis using the Signal, a media monitoring tool, suggests coverage in top media titles of AI rose 286% in the first half of 2023 compared to the preceding six months.



Bridging the societal gap

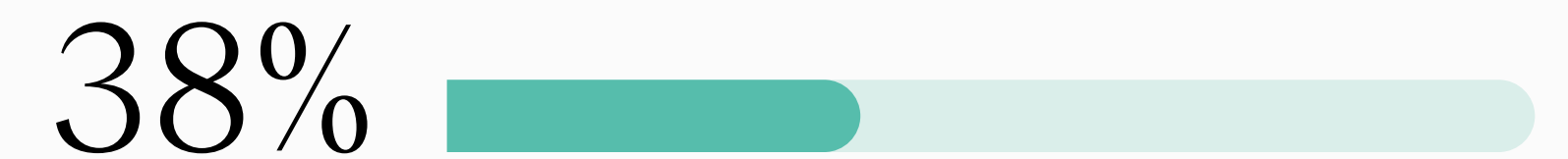
Clearly, AI is here to stay – in BSI’s Trust in AI Poll⁴ 38% of people around the world said their job involves AI on a daily basis, and it’s already firmly embedded within business operations and everyday consumer interactions such as targeted information and recommendations from the likes of Google⁵ and Amazon⁶. As our research indicates, the speed of this shift means that there could be a gap between the pace of change and the public’s understanding of it. For example, when we asked people about everyday items, we found low levels of awareness of how they currently interact with AI. For instance, 62% use curated playlists based on past listening or viewing habits (e.g., Netflix, Spotify, Amazon) – yet only 38% know these use AI.



Nearly two fifths of people are already using AI in their job on a daily basis.

Awareness is key here – helping people to understand that when they put data into systems and use certain technology, it is likely to be used by AI with the intent of providing benefit to the consumer – but there is also the potential for it to be used for other purposes, for example to sell them something.

It’s worth noting that whilst figures suggest the number of data breaches is going down⁷, the number of records being breached is going up⁸ as big tech firms – with huge volumes of aggregated consumer data – increasingly find themselves being targeted. Now is the moment to upskill the public – and fast. Mass societal education is critical to ensure AI can be a positive force for society.



An understanding gap: 62% use curated playlists but only 38% know these use AI.

Now is the moment to upskill the public – and fast. Mass societal education is critical to ensure AI can be a positive force for society

Mark Brown





AI as the cybersecurity gatekeeper

Major enterprise organizations already utilize security information and event management (SIEM) tools to monitor activity and remain alert to threats. At BSI alone, in line with other organizations of our size, we average around 150 million security log events per month (these are events related to security, such as login attempts, object access, and file deletion)⁹. For humans this is like searching for a needle in a haystack and that is the security opportunity for AI – to provide real-time data analysis based on a set of algorithms and rules which are predetermined by the controls that we operate as an organization.

The potential improvement is clear – shifting these tasks to AI could allow issues to be identified far quicker and without taking up employee time and energy¹⁰. With the right tools in place, there's the prospect of the AI analysis presenting an opportunity to take remedial action before an incident even becomes significant. This could be advantageous to organizations in all sectors. There is, of course, a critical role for humans here. In fact, our research found that people remain cautious about the use of AI for cybersecurity purposes, with 47% saying they would need to have complete or a lot of trust in AI to take on the responsibility of, for example, identifying unusual or spam email activity. In the future, the ideal situation will be cybersecurity managed as a partnership between people and AI.

Assessing the risk appetite

Against this backdrop, organizations can assess their risk appetite – do they view security as a bare minimum cost? Or, as set out by McKinsey, do they see it as a route to engaging the trust of employees, partners, consumers and institutional investors, thereby creating a competitive advantage through digital trust?¹¹

Organizations that take the long-term view may well see that, with additional investment, AI can enable them to enhance their cybersecurity, privacy or digital risk landscape and act as a proactive as well as preventative tool in their armoury. The average time to detect a breach is more than six months, according to IBM¹². Yet the company's annual Cost of Data Breach report found that AI or automation cut breach lifecycles by 108 days. In other words, AI can be a game-changer.

Organizations that take the long-term view may well see that AI can enable them to enhance their cybersecurity, privacy or digital risk landscape

Mark Brown



Not all data sets are equal

As we seek to better understand the opportunity around AI, acknowledging that there are different types of data sets can be key to unlocking their true potential.

One question to consider is: Is this data complete, or is it evolving? Identifying whether you are dealing with a fixed data set (not updated automatically), a generative data set (which learns on the go, such as Google or Amazon) or a transient data set (relevant for a limited time period such as BBC Sport live scores) means that we can assess it on its merits. Generative data, for example, may well include missing or incorrect information. The concern is that misinformation seeps through the system and gets picked up by generative AI tools¹³ – so it's important someone is taking the time to validate it. There's an opportunity for AI here to act as a filter, helping to exclude missing or incorrect information, thus driving positive progress through the dissemination of accurate information.

Organizations that put building greater digital trust at the heart of their organization's strategy are ideally positioned to thrive on society's rapidly evolving digital journey. As we accelerate towards Society 5.0, AI can play a central role in tackling cyber risks – acting as a force for good by making us safer and more secure as individuals, organizations and society.

Find out more

Mark Brown is a part of the Forbes Technology Council, an invitation-only community for world-class CIOs, CTOs, and technology executives. Read his latest industry insight and blogs [here](#).

References

- 1 Figure based on a Signal search of articles where artificial intelligence was detected as a topic in publications identified as 50 of the most influential, comparing H2 2022 with H1 2023. In H2 2022, there were 2,743. In H1 2023, there were 10,594.
- 2 [The Future of Jobs Report 2018](#), WEF, September 2018
- 3 [The economic potential of generative AI: The next productivity frontier](#), McKinsey, June 2023
- 4 BSI partnered with Censuswide to survey 10,144 adults across nine markets (Australia, China, France, Germany, India, Japan, Netherlands, UK and US) between 23rd and 29th August 2023
- 5 [9 ways we use AI in our products](#), Google, January 2023
- 6 [How Amazon uses AI to prevent damaged products from arriving on your doorstep](#), Amazon, July 2023
- 7 [Data breaches declined by almost half in Q1 2023, study finds](#), TechInformed, May 2023
- 8 [Cost of a data breach: behind the numbers of a cybersecurity response plan](#), Secureworks, July 2021
- 9 Figures from internal BSI data for year-to-date 2023
- 10 [Stay Ahead of Cybersecurity Threats by Leveraging AI](#), Aabyss, June 2023
- 11 [Why digital trust truly matters](#), McKinsey, September 2022
- 12 [Cost of a Data Breach Report 2023](#), IBM, July 2023
- 13 [How AI will turbocharge misinformation – and what we can do about it](#), Axios, July 2023



BSI Group
389 Chiswick High Road, London, W4 4AL
+44 345 080 9000
bsigroup.com

