

[Newsletter <](#)[https://techinformed.com/subscribe/>](https://techinformed.com/subscribe/)[< HTTPS://TWITTER.COM/TECHINFORMED>](https://twitter.com/techinformed)[HTTPS://WWW.LINKEDIN.COM/COMPANY/TECHINFORMED>](https://www.linkedin.com/company/techinformed) [ADVERTISE <](#)[HTTPS://TECHINFORMED.COM/ADVERTISE/>](https://techinformed.com/advertise/)**Ti** TechInformed < <https://techinformed.com>>[Home < https://techinformed.com>](https://techinformed.com) [Executive Viewpoint < https://techinformed.com/category/opinion/executive-viewpoint/>](https://techinformed.com/category/opinion/executive-viewpoint/)[Insights < https://techinformed.com/category/insights/>](https://techinformed.com/category/insights/) [Year of Elections < https://techinformed.com/category/packages/year-of-elections/>](https://techinformed.com/category/packages/year-of-elections/)

Labour's next steps: Cyber security, AI, & Open-Source industry leaders weigh in

[Executive Viewpoint](#)

Labour's next steps: Cyber security, AI, & Open-Source industry leaders weigh in

After Labour's sweeping victory in the recent UK elections, industry leaders weigh in on what Labour's tech manifesto promises mean for cybersec, AI, and open-source technology, highlighting both opportunities and challenges ahead

July 11, 2024

Following the recent change in government in the UK and the Labour Party's landslide victory, a promise of change is on the horizon.

The Labour Party's manifesto mentioned 'technology' and 'innovation' more frequently than any other party, suggesting that these will be central to the government's efforts to enhance public services, boost productivity, and revitalise the UK economy.

We've [previously discussed the promises made in the Labour manifesto < https://techinformed.com/labour-wins-uk-election-top-10-tech-manifesto-pledges/>](https://techinformed.com/labour-wins-uk-election-top-10-tech-manifesto-pledges/) as they pertain to technology in various sectors. But what are the perspectives of industry leaders on the future of UK tech policy and its potential impact on businesses?

TechInformed has gathered insights from Cybersecurity, AI, and Open-Source leaders to provide a comprehensive view of the industry's positions.

Cybersecurity & Online Safety

The election has been criticised for neglecting cybersecurity, with the industry urging the new government to prioritise cybersecurity through strong legislation, proactive strategies, and securing critical infrastructure. There are also calls to swiftly [implement and enforce the Online Safety Act < https://www.gov.uk/government/publications/online-safety-act-explainer/online-safety-act-explainer>](https://www.gov.uk/government/publications/online-safety-act-explainer/online-safety-act-explainer) to protect individuals and balance digital protections with free expression and privacy rights.

“With recent high-profile attacks on the NHS and MoD highlighting critical gaps in national security, the new leaders must play their part in ensuring that cybersecurity is a boardroom priority in all organisations with accountable outcomes, given that the UK is at high risk of a “catastrophic ransomware attack.”

“Cyber security efforts have remained stagnant even as threats rise, with 43 legacy systems at critical risk levels this year alone. The new government must take decisive action and hold all businesses accountable for improving the UK’s level of cyber preparedness through more robust and comprehensive legislation that ensures cyber security is taken more seriously.”

“Government must advocate for building cyber resilience through proactive strategies, secure-by-design principles, and visibility into everything that is coming in and out of an organisation, including encrypted data. They must also lead by example, taking steps to secure the public sector itself, especially critical national infrastructure, as the traditional IT and security strategies underpinning these organisations are no longer sufficient for the extent of today’s sophisticated threats.”

Mark Coates, VP EMEA, Gigamon

“Details from the Labour Party have been minimal. However, what we do know from their manifesto is that they recognise the threat to our safety and security. They specifically call out the growing emergence of hybrid warfare, including cyberattacks and misinformation campaigns which seek to subvert our democracy.”

“Labour proposes to tackle this by conducting a Strategic Defence Review. This will happen within Labour’s first year in government, and their manifesto states that it will set out the path to spending 2.5% of GDP on defence.”

“I urge Sir Keir and the Labour Party to speak with a broad spectrum of people across the cyber security industry, including those at the front line of law enforcement activities. The reality of the problems and the needs of the UK must be seen and addressed in this review.”

Adam Pilton, Cybersecurity consultant, CyberSmart

“For all the election noise, cyber security was absent. In a way, this is understandable; there are many other social and economic issues to focus on when trying to woo voters. But as the dust settles on this election, continuing to overlook cyber security would be a grave mistake.”

“The electoral commission: hacked. NHS hospitals: hacked. Countless UK businesses: hacked. How many attacks are too many? With Labour coming into power for the first time in 14 years, a comprehensive strategy to strengthen the UK’s cyber defences is urgently needed.”

“The EU is implementing the NIS2 directive. Why does the UK lag in securing its digital infrastructure? It’s time for the government to wake up, smell the coffee and develop a plan to change this.”

Al Lakhani, CEO, IDEE

“With the appointment of Peter Kyle as Secretary of State for Science, Innovation and Technology, it’s a vital time for Labour to reaffirm its commitment to online safety. The Online Safety Act, which Labour supported, has enabled the UK to lead the world in this space and set the direction for online platforms to make concrete changes that keep people safe.”

“The new government must ensure that the Act is not only implemented swiftly but also enforced robustly to hold tech companies accountable. Keeping up the pace here will be crucial to tackling some of our biggest societal problems, such as protecting children and other vulnerable people from age-inappropriate, harmful, and illegal content. Child Sexual Abuse Material (CSAM) and fast-developing AI-generated harms like deepfakes and nonconsensual explicit content also demand urgent attention.”

“While the focus is often on ‘Big Social’ regarding online safety in the media, we hope to see more focus on other user-to-user platforms, including video games, chat apps, and streaming services. Platforms must be held responsible for the content posted by their users to create safer online communities.”

Andy Lulham, COO, VerifyMy



Andy Lulham, COO, VerifyMy

Open Source

According to leaders in the field, the critical role of open-source technology in driving economic growth, enhancing public sector efficiency, and maintaining technological leadership calls for strategic government support and investment.

“Change must not only start now but must be digital. Only a fundamental shift in our digital policies and practices can impact the lives of every individual across the UK.

“This can be made possible by leading with digital funding the development of the right skills in open-source software. Leveraging a globally visible living CV created by open-source contribution will offer individuals who can currently code but have no employment experience the opportunity to be employed by global tech companies and hired as home workers with a proven track record of contribution.

“We should remember that these are employers who recruit based on skills, not location. In this way rurally based individuals can have international jobs, stemming talent flight, injecting international salaries into the UK economy whilst building our future tech sector.

“With 96% of software codebases having open-source software dependencies today, the public sector must learn how to manage open-source properly. Only this change allows interoperability that can open data flows between systems, unlock efficiency, and break patient and practitioner frustration in the NHS. Our new government owes the NHS this change.”

Amanda Brock, CEO, OpenUK



Amanda Brock, CEO, OpenUK

AI & Regulation

Leaders in the AI space stress the need for AI openness to prevent centralised control, urging the new government to learn from past technological developments. They emphasise tech investment, calling for the appointment of Chief AI Officers in government departments and creating an AI fund to foster public-private innovation while ensuring privacy through synthetic data.

Industry-specific regulations, especially for healthcare and pharmaceuticals, are highlighted, alongside the need for a dedicated office to ensure diverse policy input. There's also a strong call for robust AI processes to mitigate risks, ethical AI use, transparent policies, and continuous compliance to protect data and maintain public trust.

“AI will have an impact in the coming months and years like the internet in the last 20. But this time, everyone knows how the game plays out. We know the risk today is that AI ends up controlled by the hands of a few.

“This time, our new leaders must learn from the recent past. History will not be forgiving if they do not. To protect the UK's AI leadership, Labour must look to open AI wherever possible. But it must do this with a considered understanding of what that means to open each component that makes up, from models to data, and what it means to be partially or fully open.

“It's complex, yes, but we expect our leaders to be able to understand complex tasks and to cut through the distraction of the noise created by those who can shout loudest. The biggest risk the UK faces from AI today is that our leaders fail to learn the lessons of the last 20 years of tech and do not enable AI openness. Only Labour can bring this change.”

Amanda Brock, CEO, OpenUK

“It is crucial the new government places an emphasis on tech investment, particularly around AI, which will be paramount to streamlining services and enhancing citizens' lives.

“We expect to see Chief AI Officers hired across government departments to ensure AI underlines the priorities in all the parties' manifestos, while a foundational data strategy with governance at its core will help meet AI goals.

“An AI fund can also help promote public-private innovations and enable the commercialisation of data and assets globally through synthetic data. This approach would offer a unique opportunity to unlock value from data whilst maintaining robust privacy protections, as synthetic data can mimic real-world information without exposing sensitive personal details.

“Regarding AI regulation, it would be beneficial to establish industry-specific rules, with particular attention paid to sectors like healthcare and pharmaceuticals and their unique needs. For the pharmaceutical industry, in particular, there needs to be more robust agreements established on the use of medical data, with internal investment to manage and protect this data. This could include shared profits or IP rights provisions when companies benefit from UK resources.

“A dedicated office to oversee these initiatives would help to ensure that diverse voices are heard in shaping data and AI policies. These steps will be crucial for the new government to support data-driven industries and ensure they can capitalise on AI, thus positioning the UK as a global innovation powerhouse whilst ensuring sustainable growth and protecting national interests.”

James Hall, VP & country manager UK&I, Snowflake

“Labour's promise to introduce “binding regulation” for AI safety will create ripple effects across the UK private and public sectors. And while stricter regulation for major AI firms is planned, organisations leaning on these emerging technologies will have to scrutinise their AI strategy here and now.

“With Labour's wider review on the misuse of AI for harmful purposes, companies need to telegraph they are mitigating risk with AI. Both ‘good AI’ and ‘bad AI’ exist, and combatting threats from bad AI is critical in an increasing risk environment, as over half **(59%) of IT leaders say that customer-impacting incidents have increased < [https://www.pagerduty.com/newsroom/study-cost-of-incidents/#:~:text=Over%20half%20\(59%25\)%20of,customer%2Dimpacting%20incidents%20have%20increa](https://www.pagerduty.com/newsroom/study-cost-of-incidents/#:~:text=Over%20half%20(59%25)%20of,customer%2Dimpacting%20incidents%20have%20increa)**, growing by an average of 43% in the last 12 months.



Eduardo Crespo, VP EMEA, PagerDuty

“In light of regulation pressures and mounting risk factors, companies need to establish watertight AI processes and mechanisms to ensure the ethical use of AI; how are external AI threats being tackled? How are internal hygiene processes with AI protecting customers? CIOs and DPOs face a big set of tasks involving sticking close to regulators, sharing rigorous policy documentation publicly, and implementing clear and transparent network policies on data collection and information security.

“Compliance is a 24/7 job, and dropping the ball on this, with regards to areas like data protection, could result in hefty fines and loss of trust.”

Eduardo Crespo, VP EMEA, PagerDuty

For more tech-oriented coverage of elections around the world, check out our dedicated hub to the [Year of Elections < https://techinformed.com/yoe-lp/>](https://techinformed.com/yoe-lp/).

[AI < https://techinformed.com/tag/ai/>](https://techinformed.com/tag/ai/)

[CYBERSECURITY < https://techinformed.com/tag/cybersecurity/>](https://techinformed.com/tag/cybersecurity/)

```
< https://twitter.com/intent/tweet?
< https://www.linkedin.com/shareArticle?
< text=Labour's next steps: Cyber security,
mini=true&url=https://techinformed.com/labour-
https://techinformed.com/labour-
promises-tech-insights-cybersecurity-ai-open-
source/&title=Labour's next steps: Cyber security,
AI, & Open-Source industry leaders weigh in>
open-source/&via=WPCrumbs>
```

ABOUT THE AUTHOR

Ricki Lee

Suggested Articles

[Labour's next steps: HealthTech, GreenTech, and Startup industry leaders weigh in](https://techinformed.com/uk-election-2024-health-tech-green-tech-economy-startups-productivity/)

[< https://techinformed.com/uk-election-2024-health-tech-green-tech-economy-startups-productivity/>](https://techinformed.com/uk-election-2024-health-tech-green-tech-economy-startups-productivity/)

by Ricki Lee

[Navigating the rollout Gen AI in enterprise](https://techinformed.com/navigating-the-democratisation-of-generative-ai/)

[< https://techinformed.com/navigating-the-democratisation-of-generative-ai/>](https://techinformed.com/navigating-the-democratisation-of-generative-ai/)

by Techinformed admin