trowers & hamlins

Thinking Business

Issue 14

Contents

Introduction

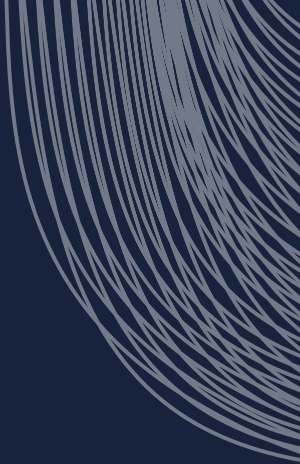
Welcome to Issue 13 of Thinking Business, a Trowers & Hamlins bi-annual publication in which we share our latest insights and commercial thinking to help businesses adapt, grow and be successful in a rapidly changing world.

In this edition of Thinking Business:

AI strategy: Plugging the governance gap – AI has unlimited potential across almost every industry. However, legal and commercial issues pose challenges. What can you do to avoid risks and disadvantages at your company?

Shaping up to address cyber risk – In the fast-paced digital world, data breaches and cyber-attacks weigh heavily on business leaders. We speak to Stuart Hadley, CEO of CyberQ Group about the launch of our joint CyberSecure360 service and to discuss the need for a cyber strategy in this ever-growing digital world.

Effectively deploying AI in recruitment – Advances in AI tools have been so rapid that many businesses have found it is their HR and People teams that are at the cutting edge of decision-making. But what's the best way to use AI when recruiting new employees?



AI STRATEGY : PLUGGING THE GOVERNANCE GAP

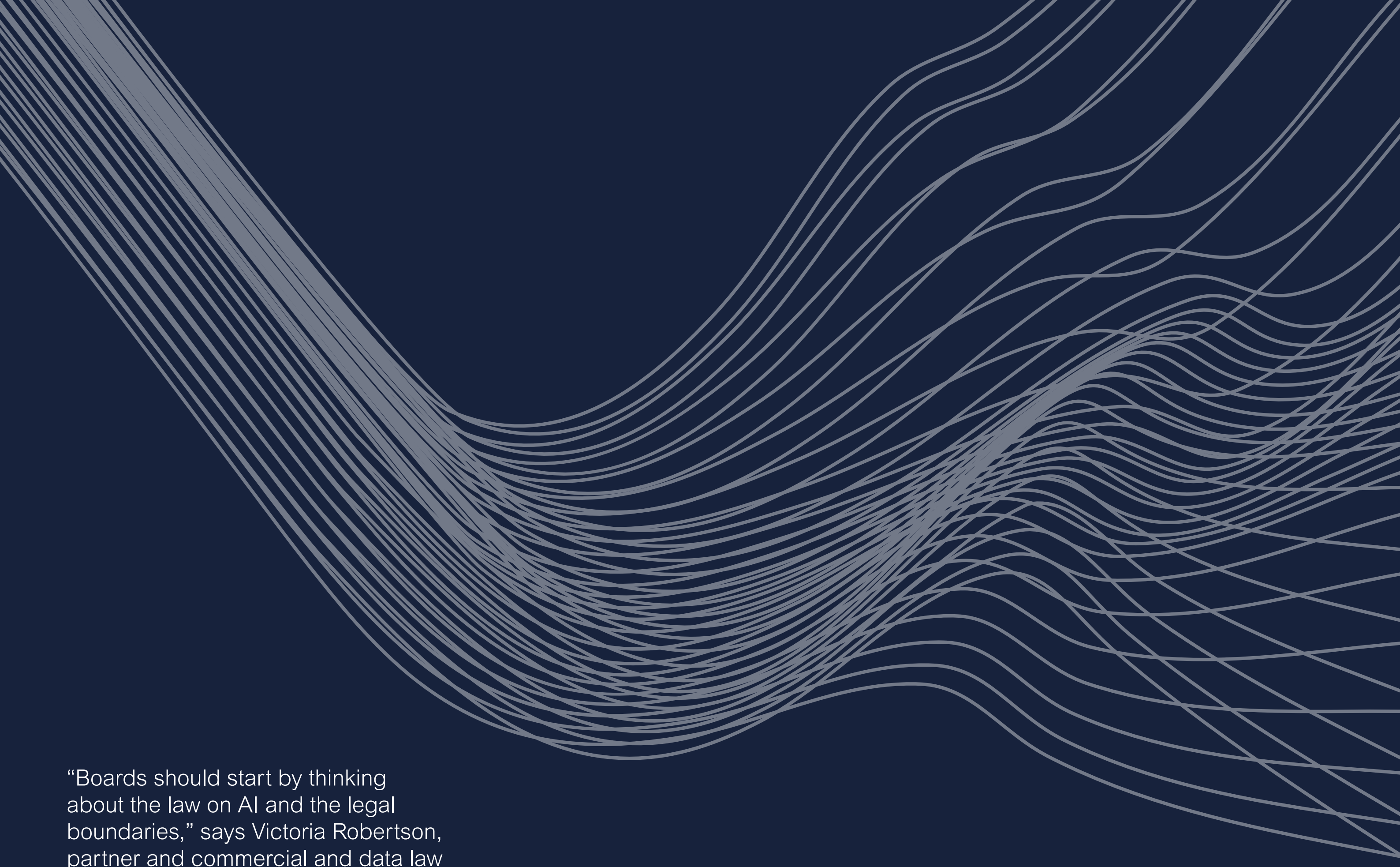
If you're not already using artificial intelligence tools within your business, the chances are you are at least thinking about doing so. Ever since ChatGPT swept into our everyday conversation a year ago, there has been an arms race for the top spot in the AI community – Google's Bard, Meta's LlaMa and BingChat are all competing with Open AI at a rapid pace of innovation. The number of generative AI use cases has proliferated and it is likely that most of your employees have dabbled with testing one or two.

AI has unlimited potential across almost every industry. Human resource professionals are increasingly discussing the ability of AI tools to speed up candidate selection processes and identify potential high-performers. But beyond that, there are opportunities springing up that could enhance every company in every sector: restauranteurs are using AI to advise customers on the wines they will like, doctors are using it to identify when non-verbal patients are in pain, and elderly care homes can employ it to match residents with common interests so that they can enjoy social interaction.

Microsoft's new AI assistant Copilot is now generally available to business customers, promising another wave of AI adoption. "Not every company will sign up to Copilot, but many will," says Anna Browne, head of innovation and legal technology at Towers & Hamlins.

> **"With many suppliers integrating generative AI into their existing products, we can expect a big shift in the number of businesses embracing AI to help drive productivity and growth."**

The challenges arise when it comes to thinking about the many legal and commercial issues that might arise as a result of AI adoption – careful attention needs to be paid to making sure employees only use AI in a way that is sanctioned, and that no one inadvertently brings risks or disadvantages to the company's door.



"Boards should start by thinking about the law on AI and the legal boundaries," says Victoria Robertson, partner and commercial and data law specialist at Trowers. "The problem is that right now we don't have any specific laws on AI in the UK. That was a big focus of the AI Safety Summit in the UK in November, which was the first global event of its kind looking at how best to manage the risks from advances in AI."

At the same time, the UK government launched the world's first AI Safety Unit to examine, evaluate and test new types of AI, and it has also significantly expanded its AI Taskforce by recruiting a growing team of researchers. But regulation has so far been unforthcoming and inconsistent all over the world – the European Union's AI Act is the most advanced attempt at a rulebook but we do not know when it will come into force, and the US AI Bill of Rights is nothing more than guidance for now.

For now, businesses only really have the General Data Protection Regulation (and its UK equivalent, UK GDPR) to govern how personal data can be used in AI algorithms.

Browne says: "Everyone wants to understand the parameters of what they can and can't do, but because there are no specific AI laws to comply with it is tricky to navigate at the moment.

> **Without clear rules, the need to set out clear guardrails for use within your organisation and to put in place strong internal governance to plug the regulatory gap is critical."**

So what practical steps can you take to protect your business from potential AI mis-steps?

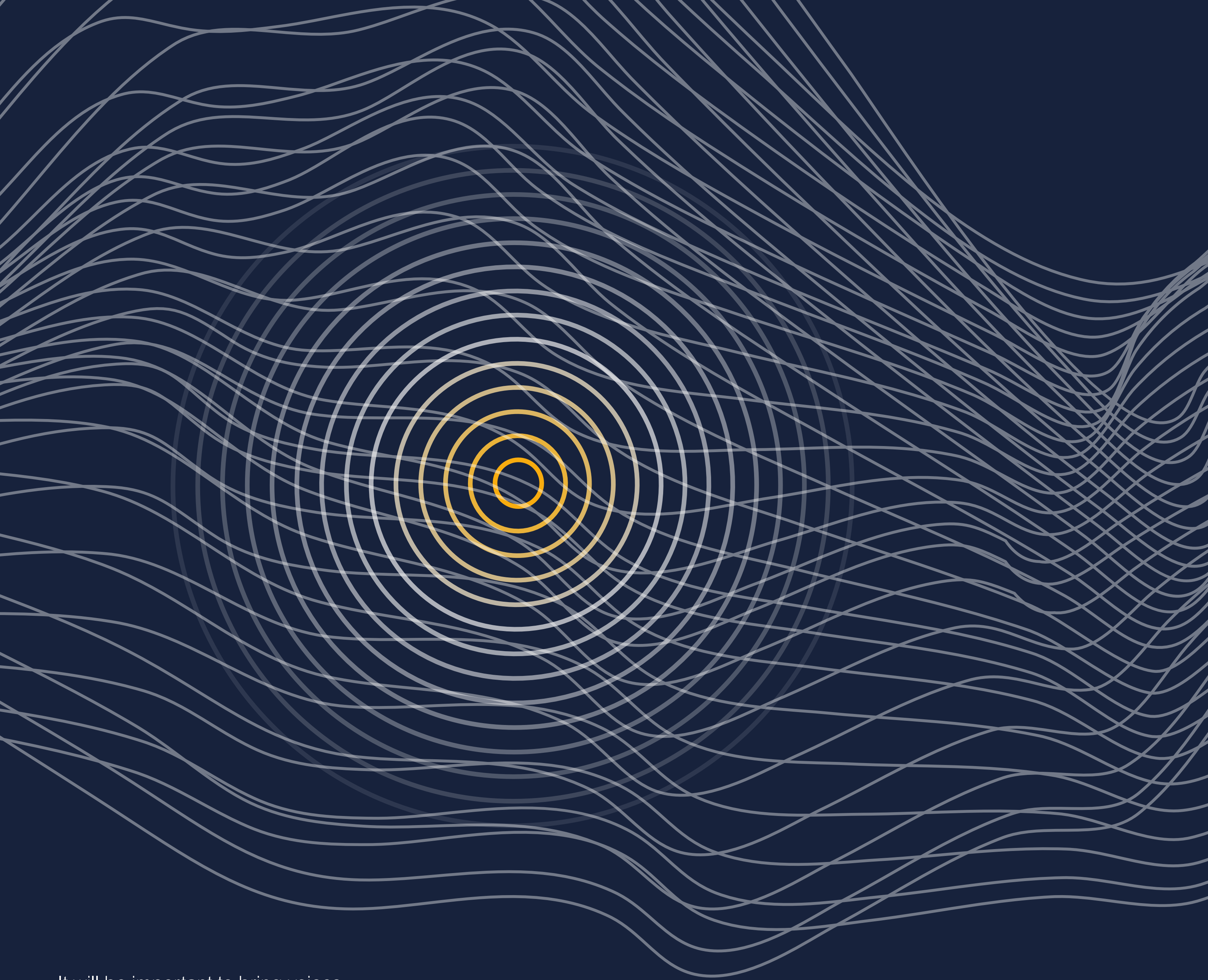
First, before you buy an AI tool, do your due diligence on suppliers. It is vital to dig into the detail of how the AI has been trained, whether the data being used is proprietary or if the tool is opensource and whether there has been an ethical approach to the harvesting of that data.

Any AI tool should be implemented in line with the company's data strategy. Protecting your data and that of your customers is essential. UK GDPR already dictates that data should be held by design rather than by default and the same approach should be taken when using AI.

Another consideration will be the extent to which any professional indemnity insurance covers the use of AI, and that should be looked into.

Your corporate AI strategy will need to be agile because both the technology and the regulatory environment are evolving fast. We would therefore recommend that clients set up AI governance groups to keep things under review and take responsibility for AI governance across the business.

Members of that governance group should be your innovators, knowledge owners, likely including people that work with AI in their day-to-day roles, such as the IT director, knowledge management director and general counsel. People coming from different workstreams will also bring their own insights, so HR should also be involved to add input around the risk of discrimination that can be embedded with AI tools.



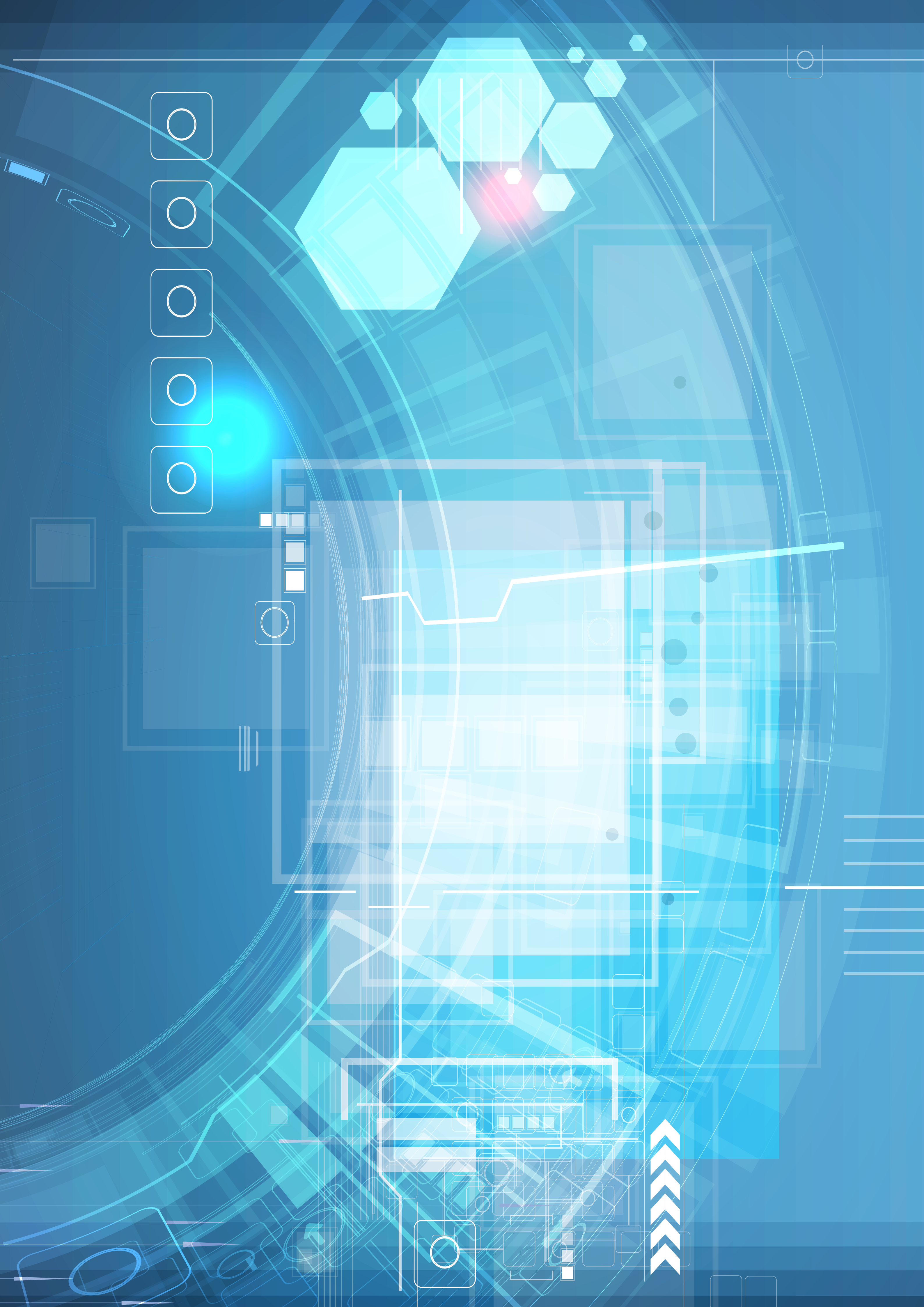
It will be important to bring voices together at that table who will identify opportunities as well as risks and who will not be too risk averse. The adoption of AI should add additional resource and capability to the business, rather than simply being about cutting headcount or reducing cost.

Another practical point is to focus on employee engagement around AI, because it is really important to have open dialogue on this. Some members of staff will be more comfortable with new tools than others and some will be wanting to use it while others won't – leaders should ensure there is proper, balanced oversight and that an environment is created in which people can ask questions and explore opportunities collaboratively. We are already seeing demands for more accountability in AI adoption, for example with public authorities asking for assurance that AI has not been used in procurement documents.

Robertson says: "We can already see that employee attitudes to AI are changing, and people are less frightened of losing their jobs and more focused on ways in which they can make use of ChatGPT and similar tools work for them.

For businesses, it is important to set the boundaries of what is considered to be acceptable use within the workforce, and communicate those boundaries effectively whilst not stifling innovation."

The vast majority of UK businesses are yet to put effective AI governance in place but there are many questions that organisations looking to future-proof their operations need to address. Trowers recently launched a new AI Strategy Toolkit to help leaders identify issues relevant to their businesses and create workplace policy guidance tailored to those needs. Please get in touch if you would like more information.



Shaping up to address cyber risk

In the fast-paced digital world, the risks associated with data breaches and cyber-attacks weigh heavily on the minds of all business leaders.

The UK government estimates as many as 2.39 million instances of cybercrime have impacted UK businesses in the past 12 months. High-profile attacks continue to hit the headlines. In the Summer, Boots, British Airways and the BBC were hit with an ultimatum from a Russian-speaking cybercrime group to begin ransom negotiations after it stole personal details of more than 100,000 of their staff. Similar attacks are happening every day in small and medium-sized businesses around the country.

"There is a lot for businesses to deal with at the moment," says Elizabeth Mulley, managing associate in Towers & Hamlins' dispute resolution team. "Along with geopolitical unrest, energy prices fluctuating and high inflation and interest rates, there is also an increased dependence now on technology. Businesses are sometimes making large investments in new technology and new communication platforms in a rush, and that can leave them vulnerable. When there is so much to focus on in the day-to-day operations, the risk is that they leave the back door open to hackers and cyber criminals."

The conflicts going on around the world have demonstrably increased the risks of cyber-attacks and put companies under even more pressure to prioritise cyber security. While many have focused their efforts on responding to breaches once they happen, there is a lot that companies can do to mitigate risks and address vulnerabilities to prevent becoming a target for cyber criminals but also to minimise loss and impact suffered if they are exploited.

A solid cyber strategy encompasses not just investment in technical skills and capabilities, but also in governance and compliance. That is why Towers has launched CyberSecure 360 with cyber security company, CyberQ Group – together our goal is to help clients comprehensively manage cyber risk by combining technical and legal expertise. CyberSecure 360 offers a range a bespoke services that span the entire cyber risk management spectrum, including pre-breach preparedness and post-attack assistance.

"This is about raising awareness and getting ahead of issues," says Stuart Hadley, global group COO at CyberQ Group. "Rather than simply being reactive, companies need to raise the level of C-suite and employee understanding of these issues, putting cyber security at the top of the priority list. This is a whole business problem. We often see it sat within IT as their responsibility, but in fact it cuts across everything; it is to do with supply chains, attracting new customers, company insurance, M&A due diligence and much more.

Addressing cyber security is a key element of building resilience in any business and just leaving it to IT is a bad plan."

He adds: "There also needs to be a shift in culture away from the view that 'it won't happen to us'. Even if you are a small business, you will be a target for hackers trying to get at bigger businesses. As attackers get more sophisticated, they are doing more reconnaissance and being more strategic in who they target and why."

While it might be the big hacks on multi-billion pound companies that hit the headlines, these attacks are happening in small businesses, charities and schools all the time, so it is not a question of if but rather when your company might be in the firing line. Still, by developing your cyber readiness and building defences in advance, enduring an attack can be much less costly and disruptive than it might otherwise have been.

"The first step for any company is looking at and considering your security threats," says Mulley. "You need to understand your vulnerabilities, the risks those represent and the likelihood that they can be exploited. Then you can assess your internal and external safeguards already in place and see where the gaps lie, before moving on to plugging those gaps and building up resilience."

Hadley adds: "Doing that gap analysis helps people spot risk priorities and allocate resources effectively to the areas of most concern. And it is important to consider what the impact will be if a breach does happen. The perception is that cybersecurity is expensive but it's not when you put it into the context of the threat to the company. For most people,

investing in a vulnerability assessment and then the right policies and procedures can put them in a much better position to recover quickly from any incident."

Helen Briant is a partner in the Trowers disputes team. She says: "The thing companies underestimate is the potential damage to their reputation of an attack. You can figure out in pounds and pence what might be the impact of your output being disrupted for a week, but if your customers walk away because they have lost faith in you, that will take a lot longer to recover from."

Hadley says that clients may be faced with paying a £500,000 ransom and be tempted to hand over money to get systems back up and running, but that is rarely the best way forward. In all likelihood, hackers will leave something in systems to allow them to come back for more, so again the impact is more far-reaching than might be immediately evident.

Having completed a thorough cyber risk assessment, the next step is for companies to build a practical cyber risk management strategy. "That is about setting clear objectives around what you aim to achieve and then setting the wheels in motion," says Hadley. "We are trying to get companies to bring in cybersecurity support every time they start a new project, on day one, because too often people get halfway through something and then realise they forgot about this."

Mulley says a good cyber risk management strategy is revisited and monitored frequently, to make sure it stays a priority and keeps up with evolving risks. It will bring together legal and technical skills to encompass everything from risk assessment and gap analysis through to legal compliance, policies and procedures, awareness training, cyber insurance and investment in technology where appropriate.

A comprehensive strategy will also set out a clear incident response plan, including a communication plan for employees, customers and stakeholders in the event of an incident and a strategy for ensuring regulatory bodies are informed within the 72-hour reporting window.

She adds:

"There is no one-size-fits-all approach to this. There has to be time put into tailoring the strategy to meet the needs of your organisation and your industry, because every business will have different vulnerabilities."

The government's National Cyber Strategy is focused on helping companies build a more cyber resilient future and is starting to bring out frameworks and guidance for businesses to follow, though there are currently no legal requirements. "We think that's coming," says Hadley. "There has been talk about the UK government introducing standards that organisations must comply with – for now, it is just asking companies the difficult questions."

The key takeaway is that cybersecurity needs to be embedded into the fabric of a business, as everyone's problem. Hadley says: "It doesn't matter who you are, what kind of business you are, where you are or what size you are, everyone is prone to being attacked. There are lots of people surveying the internet looking for holes, just like thieves walking the streets looking for car windows left open."

We have launched CyberSecure 360to help our clients enhance their cyber resilience and ensure that they have the necessary safeguards in place to counter evolving cyber threats should an incident occur.

EFFECTIVELY DEPLOYING AI IN RECRUITMENT

As the buzz about artificial intelligence has been gathering pace, with the potential to transform countless aspects of our personal and professional lives, the recruitment industry has found itself at the sharp end of new technology adoption.

Advances in the AI tools available to help companies source, recruit and retain staff have been so rapid that many businesses have found it is their HR and People teams that are at the cutting edge of decision-making on how such tools should be deployed.

Time-saving algorithms that are capable of communicating with candidates on behalf of companies, of shortlisting candidates and of setting up their interviews have been around for some time, bringing with them a raft of discrimination bias risks that companies are becoming more aware of.

Now the next generation of tools goes further, with the ability to write job specifications by identifying what is missing from an existing team, for example, or to assess not just the technical fit of a candidate but also their personality fit, to tell you whether they'll work well in your business. This presents a whole new range of challenges for employers looking to seize opportunities without tripping up.

Nicola Ihnatowicz, a partner in the employment department at Trowers & Hamlins, says: "There were some horror stories in the early days of AI recruitment, when employers' models didn't shortlist any women, for example, because they were relying on data on who had made it to the top of the tech industry in the past decade."

Companies are now aware of those challenges and much more mindful of ensuring algorithms combat bias and are properly overseen, she says.

But from a business point of view, Ihnatowicz says there are now several risks.

"The first one is that the technology is moving so fast that it's hard to keep up and understand what the tools are doing and what their impact might be," she says. "That is not a reason not to get involved, but it is really important that a business understands what a tool is doing and what the company is trying to achieve with it."

On discrimination risk, she adds: "That is something businesses need to be alive to, and I think they are. But that doesn't mean we can assume all tools are okay. You have got to actively engage on this, talk to your AI provider, understand the technology and be inquisitive about the results, asking about the underlying data. If you are implementing something, you need to keep reviewing outcomes, so that you are aware if you are accidentally ending up with results skewed by age, gender or ethnicity, for example, and then you can make changes to stop that happening."

When it comes to the latest generation of tools capable of assessing the cultural fit of a candidate, and even who they might best work alongside within the business, Ihnatowicz says it is important to be aware of unintended consequences.

"You might want to use terms like 'a structured working environment' to differentiate a professional services firm from a start-up tech business, which is fine, but you want to make sure that the AI doesn't screen out people who might need flexibility for reasons such as childcare responsibilities as a result, or people with long commutes," she says.

Danielle Ingham, also a partner in the employment and pensions team at Towers, adds: "One potential problem is, what does "cultural fit" actually mean? Looks like everyone else? Has similar background and interests?

You really have to make sure you are using the technology as a solution for greater inclusion and not unintentionally exacerbating problems. It's actually a great opportunity for employers to tailor something bespoke and be really thoughtful about that, challenging the requirements in the same way that they would in a traditional recruitment process."

Anthony Kelly, the founder of AI and blockchain recruitment specialists DeepRec.ai who recently joined one of our Trowers Tuesday sessions on being a Digital Employer of the Future, says: "The key is to always keep a human in the loop. Whatever process you introduce to automate and make your processes easier, having someone who can say this isn't quite right or we're not getting the desired results is the best way to achieve the right alignment with the business and the HR strategy."

There are many great examples of high tech algorithms making a positive impact to combat employment bias, including through the use of contextual recruitment tools. At Trowers & Hamlins, we have started using a contextual recruitment tool as part of our graduate recruitment process, as it enables us to identify the best hires from the widest possible pools of candidates.

The software that we use allows us to assess candidates' achievements in the context of their background. We ask applicants to fill in an entirely optional form at the outset of the process, which asks questions about the schools they attended, whether they were eligible for free school meals, whether they have ever spent time in care, and much more.

It then produces a social mobility output for a candidate and a performance metric, showing how well someone did in their A-levels compared to every one else in their school, or their town, and highlighting the extent to which they have outperformed their peers.

Rachel Chapman, graduate recruitment and development manager at Trowers, says: "We might look at someone who got ABB in their A-levels and pass them over, but if the average at their school was DDD then we don't want to miss them out. It is very much about screening in rather than screening out, and candidates absolutely win their places with no lowering of standards."

She adds: "We look for resilience, determination and drive in our graduate recruits and candidates that have outperformed their peers are much more likely to have those attributes. Recent studies show outperformance at school is likely to lead to outperformance at work."

Ihnatowicz says the key to success with all these recruitment tools is making sure a human takes the final decision. "That means you also have to be wary of confirmation bias," she says.

"Just because the computer says something, that doesn't make it right.

The other takeaway is to always be critical of the results and keep models under review so that you can keep making improvements."

trowers & hamlins

trowers.com

Printed on sustainably sourced paper without the use of water or volatile organic compounds by net zero carbon printer Seacourt Press Ltd.