trowers & hamlins

Thinking Business

Issue 17

Contents

Addressing new cyber risks created by AI 4

Ethics of AI in the workplace 8

Managing transformative change through leadership 12

© Trowers & Hamlins LLP. This document is for general information only and is correct as at the publication date. Trowers & Hamlins LLP has taken all reasonable precautions to ensure that information contained in this document is accurate. However, it is not intended to be legally comprehensive and it is always recommended that full legal advice is obtained. Trowers & Hamlins assumes no duty of care or liability to any party in respect of its content. Trowers & Hamlins LLP is an international legal practice carried on by Trowers & Hamlins LLP and its branches and affiliated offices – please refer to the Legal Notices section of our website https://www.trowers.com/legal-notices

For further information, including about how we process your personal data, please consult our website https://www.trowers.com

Introduction

Welcome to issue 17 of Thinking Business, a Trowers & Hamlins publication in which we share our latest insights and commercial thinking to help businesses adapt, grow and succeed in a rapidly changing world.

In this edition we look at how those in leadership can empower their businesses to thrive, from the rapid advances in technology which may threaten cybersecurity to the growing importance of empathetic leadership.

Addressing new cyber risks created by AI – with what seems to be weekly headlines of major corporations being hacked with painful cyber-attacks, we look at how to recognise the risks within your business and how those in leadership can build resilience through their staff.

Ethics of AI in the workplace – AI is steadily being used more and more by staff, and in this article we examine how leaderships can lean into its transformation of the workplace without putting important issues at risk, such as GDPR.

Managing transformative change through leadership – To close this edition, we welcome back Sahar Hashemi OBE, co-founder of the consumer movement Buy Women Built, alongside Sara Bailey, Senior Partner at Trowers. Together, they explore what it means to be an empathetic leader in today's unpredictable world.

We hope you'll enjoy reading this and that you'll find some interesting food for thought over the course of the following pages.

Addressing new cyber risks created by AI.

The cyber threat landscape is changing all the time and rarely a week goes by without a major corporation hitting the headlines as a result of hackers executing painful cyber-attacks. This year has seen Marks & Spencer, Co-op and Jaguar Land Rover all fall victim to extremely costly and disruptive incidents, and the role of technology in escalating the threat level cannot be underestimated.

Friend or foe: the role of tech

While geopolitical forces are inevitably playing a significant part in elevating cyber risks, the ability of technology to power bad actors is turbo-charging a fast-growing threat level. While new technologies like AI and generative AI can do much to support businesses as they look to more proactively identify and detect threats and build cyber resilience, there are several ways in which the tools are also raising risk.

For a start, AI tools allow hackers to automate some of their attacks and to scale their attacks in both number and impact. Given these malicious individuals are seeking financial reward, this heightens their success rate.

At the same time, new technologies lower the barriers to entry for criminals, meaning even novices can create malware and ransomware with the support of AI tools. The National Cyber Security Centre has noted an increased pool of individuals that now has access to the ability to hack systems.

AI helps criminals make cyber attacks more sophisticated and therefore more effective. However much businesses train their people to look out for dodgy email addresses or other signs of phishing emails, when hackers can scrape the internet for video footage of a CEO and then have a deep fake of that individual show up in a Teams meeting, that becomes incredibly hard to spot.

Charlotte Clayson, Partner in the Dispute Resolution and Litigation team at Trowers & Hamlins, has extensive experience helping businesses both prevent and respond to cyber-attacks. She says:

“It is quite easy to receive a voicemail from your colleague in the finance team, or attend a video call with them, and believe them when they ask you to transfer money. That is the most tangible example of AI for bad.”

We know that the recent M&S cyber attack involved a sophisticated impersonation, where the attackers posed as legitimate employees and were able to trick IT help desk personnel into resetting passwords and essentially unlocking the systems for them.

That attack cost the retailer an estimated £300 million in lost revenue as it raced to recover its systems. Meanwhile, the estimated impact of the cyber-attack on Jaguar Land Rover was £1.9 billion, making it the costliest cyber incident in UK history, disrupting the company’s manufacturing for weeks and affecting over 5,000 companies across its supply chain.

Clayson says: “Businesses have long been concerned about data leaks but we are increasingly seeing the operational impact of cyber-attacks having the potential to create much more immediate and devastating financial impact. AI is a good thing for the good guys, but also a good thing for the bad guys.”

She adds: “As more and more businesses bring on board new technologies, there is a need for enhanced awareness of the vulnerabilities coming into systems.”

Recognising the risks

Data from the latest Cyber Security Breaches Survey, published by the UK government, highlights the fact that 72% of businesses consider cyber security a high priority for their senior management. However, only 27% have a board member with responsibility for cyber security, and that figure has declined from 38% in 2021.

Further, the survey reveals that only one in five organisations provide training to their staff on cyber resilience, despite training also being the most common preventative measure that businesses adopt following an attack. That just shows

the importance of being proactive in addressing cyber risk.

But perhaps the most important thing that organisations can do to build resilience is set a tone from the top that elevates cyber safety and instils a culture of taking these threats seriously.

"Whenever I talk to businesses about cyber-attacks and how to protect themselves, I always start with the importance of strong leadership,"

says Clayson. "Technology is developing at such a rate that most businesses cannot realistically keep up with the threats that are out there, so they can't remove all the risks. What they can do is actively engage with the issue and think strategically about how to manage it."

It is easy for companies to think about cyber resilience as an issue for the IT team or for information security specialists, but siloing responsibility is not the best way to protect themselves.

Strong leadership starts with building a tangible understanding of what the risks look like for the business in question, because every firm has different priorities and vulnerabilities. While Jaguar Land Rover exposed the threat of widespread disruption across a supply chain, the recent attack on nursery chain Kido International highlighted what can happen when hackers steal sensitive data – they took names, addresses and photos of approximately 8,000 children.

Once the board has fully grasped the financial, operational and reputational risks that cyber threats represent, the next step is mitigation and putting in place a response plan to deal with any attack that unfolds.

The UK Government has published a Cyber Governance Code of Practice that sets out around 20 action points for boards to take in order to most effectively govern cyber risk.

"That code covers questions boards should consider in relation to risk management, strategy, people, incident planning, response and recovery, and assurance and oversight," says Clayson.

"It is a really good place for people to start if they are trying to get on the path to cyber resilience."

A cultural imperative

By prioritising leadership, businesses can ensure their people engage with cyber risk and the right attitudes and behaviours trickle down through the organisation. Staff need to be empowered to report things that they think are concerning and to make suggestions where they think processes and procedures might be strengthened.

"An open and transparent culture has to be led from the top," says Clayson,

"empowering everyone in the organisation to take small steps to really protect the business. Phishing attacks involve a huge human element – only when people know what to look out for and how to respond can you really make an impact."

If a business does fall victim to a cyber-attack, the first 24 hours are critical. And yet despite so many businesses having cyber risk at the top of their risk register, the Cyber Security Breaches Survey shows only 30% of businesses have a formal incident response plan in place.

"You need to have a response plan, know who the decision-makers are at every level, and then practice that in a simulation," says Clayson.

"You can work through a realistic attack scenario in an afternoon, including people from across the business – HR, finance, legal, regulatory, customer facing and IT."

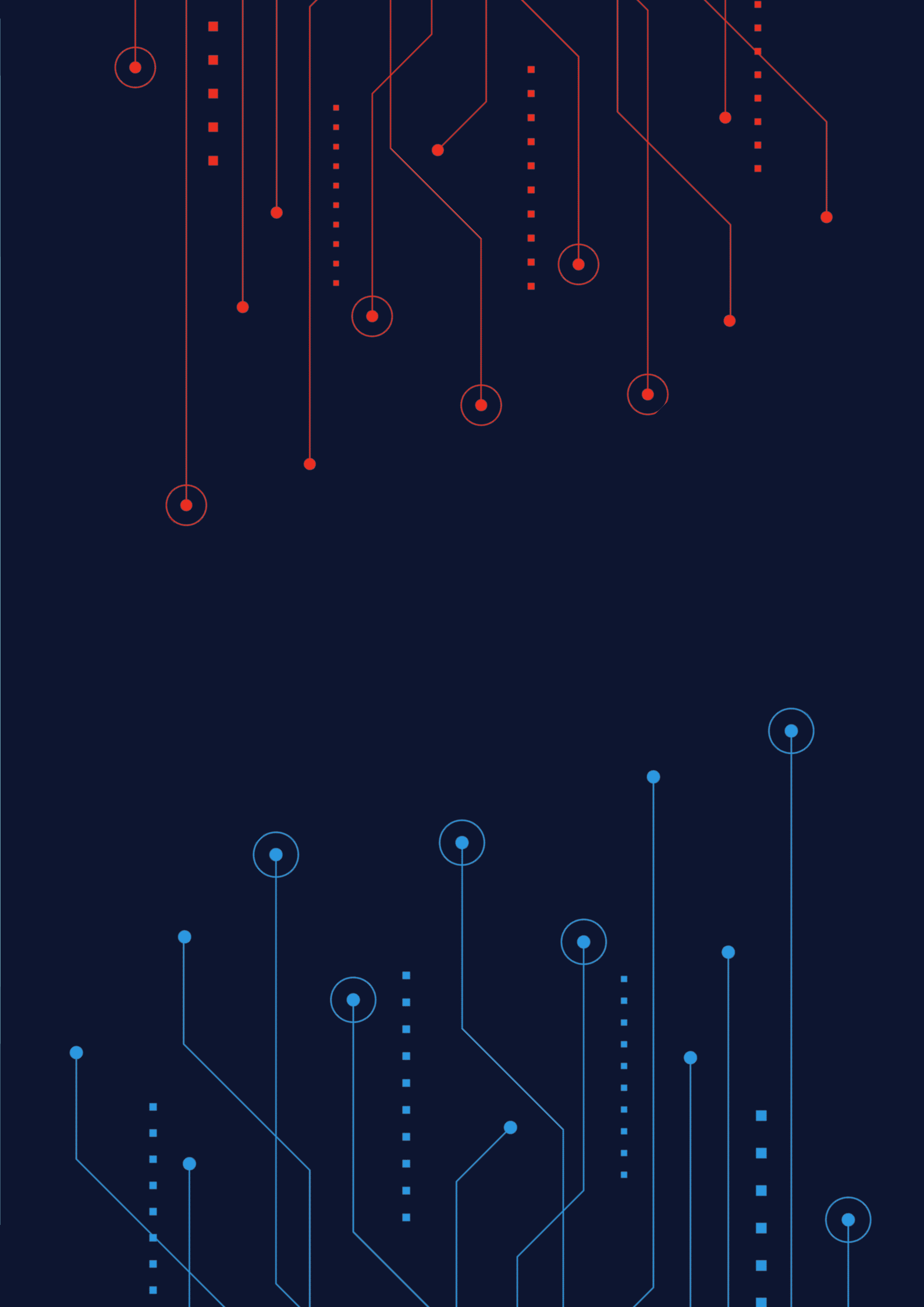
She adds: "Bring those teams together because everyone will see things from different angles, and you can walk through all the decision points along the route and discuss competing priorities. That puts the whole business in a much better position."

Best practice dictates that the incident response plan, once formulated and agreed, should exist in hard copy somewhere on the business premises – too often companies overlook the fact that it will otherwise be hard to access when systems are down.

There is no denying that cyber security can be technical, expensive and frightening. But instead of allowing that to result in a lack of engagement, senior leadership teams need to lean in and take a proactive approach to managing the risks.

"So much of being cyber resilient is about understanding the risk, engaging with it and making sure you have a plan and a culture to respond and recover as quickly as possible," says Clayson.

Technology may be elevating the threat, but companies still have the power to respond.



ETHICS OF AI IN THE WORKPLACE

There are plenty of reasons to be concerned about the arrival of AI in the workplace, not least because its advent heralds a new era of transformational change for leaders and employees to navigate. Further, the headlines about AI taking over professional services jobs and replacing staff with chatbots and datasets are plentiful and hard to ignore.

But cutting through the hype to understand the present realities is important, particularly as businesses look to reassure workers and move forward thoughtfully with their AI implementation and technology strategies.

The first thing to accept is that AI is here to stay: there is little option for most companies but to explore its potential and embrace its use where it makes sense to do so. "AI will be transformative," says Amardeep Gill, Partner and Head of the Public Sector Practice at Trowers & Hamlins.

"But it will be transformative in the same way that email and the internet were transformative before it, although the pace of change is far greater. Leaders need to both understand the technology and its application and help their teams to adapt."

Unemployment hit 5% in the UK for the three months to September 2025, the highest rate since the period covering December 2020 to February 2021. Particularly hard hit has been graduate entry level roles, where job postings have fallen from 180,000 four years ago to just 55,000 today, according to job platform Reed.

And yet while many have blamed AI for that employment decline, the truth is more nuanced, says Rebecca McGuirk, Partner and Head of Employment and Pensions at Trowers:

"There are many reasons why graduate recruitment is low at the moment, many of them associated with economic uncertainty and rising costs. Certainly, businesses may be looking at how tech can help with addressing those challenges, but an investment in tech is expensive too – it is no cheap quick fix."

The impact of macro issues on employment data is being conflated with concerns about AI eroding jobs, says McGuirk. She also points out that research increasingly indicates the new technology will not have such a dramatic impact as some fear on the job market

Research from Goldman Sachs suggests that, while innovation related to AI could displace 6 to 7% of the US workforce if AI is widely adopted, the impact is likely to be transitory. New job opportunities will be created as the technology ultimately puts people to work in new capacities.

"A recent pickup in AI adoption and reports of AI-related layoffs have raised concerns that AI will lead to widespread labour displacement," Joseph Briggs, who co-leads the Global Economics team in Goldman Sachs Research, and economist Sarah Dong, wrote in that report.

"While these trends could broaden as adoption increases, we remain sceptical that AI will lead to large employment reductions over the next decade."

Developing an ethical AI strategy

After dispelling myths and reassuring workers, the next step for many business leaders will be an AI audit to identify both the threats and the opportunities that new technologies might bring to their organisation. Those impacts will vary enormously from one industry to another, and from one business to the next.

"What we are seeing is that AI is disproportionately affecting professional services,"

says Gill. "Just as blue collar workers were impacted by automation, so professional advisers are impacted by a new unprecedented access to knowledge and perceived wisdom. However, the provision of knowledge is only one part of what an adviser does, and AI cannot fully replace strategic guidance, corporate expertise or implementation experience."

Many businesses will identify potential efficiency gains and time savings that can be delivered through AI adoption. "It gives you the ability to look through a lot more data," says McGuirk.

"Because it can summarise large amounts of data, leaders can keep abreast of far more sources of information and have far more data feed into their decision-making."

Businesses are tackling both understanding what the technology can do and navigating a successful roll-out. When completing an audit to identify potential use cases, employees should be part of the conversation, not least because different teams will see different applications, ranging from document review to data processing.

Once use cases and tools are found, a clear policy is needed to govern implementation. Gill says:

"Businesses will need AI strategies that tackle some of the big issues around transparency, accountability, regulatory compliance and fairness. When buying a product, organisations need to understand the algorithms on which decision-making is being based, as there can be a discrimination risk there."

Where AI is used to sift through job applications, for example, it might introduce unconscious bias into decision-making if it has been trained to look for certain keywords. There is evidence that men use different language when completing job applications to women, so a tool trained on male applicant responses may inadvertently disadvantage female job seekers.

Similarly, it is important employees are using the right tools and using them properly, so that confidential business data, or personal data relating to customers, does not get shared on open platforms.

Then there is the regulatory angle to keep close watch over. "We have a real patchwork regulatory framework in the UK as it relates to AI," says Gill.

"You need to be mindful of GDPR, the Equalities Act and the new Employment Rights Bill. Those will all have an impact on how AI can be used in the workplace."

Lean in or get left out

AI adoption certainly does not come without complexity, but that is no reason to stay away. "The onus is on the business to lead," says McGuirk, "because otherwise you risk your people using it incorrectly and losing control of your data, which can give rise to significant reputational damage as well as penalties from the Information Commissioner's Office."

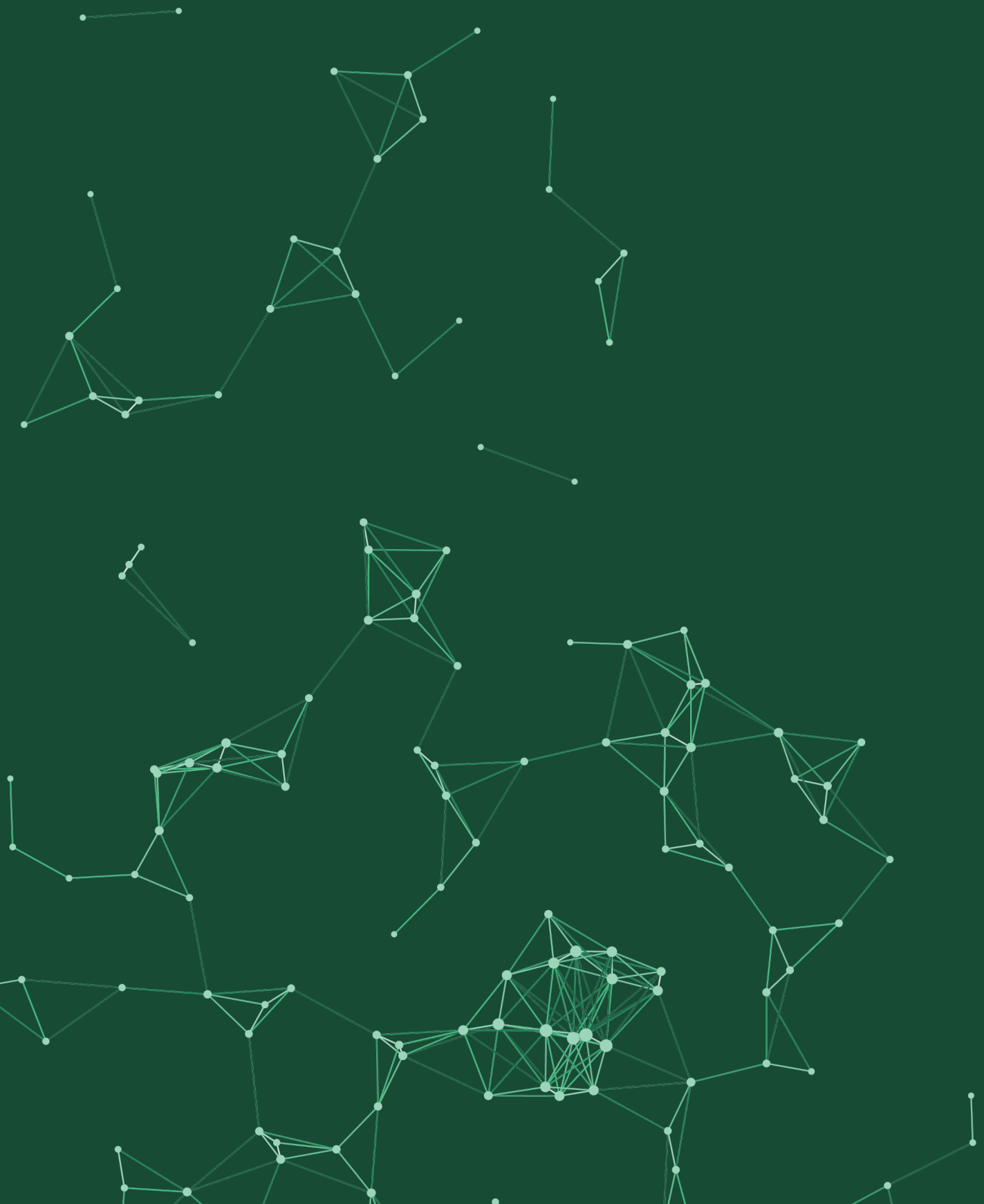
A report by Microsoft published in May 2024 found that 75% of global knowledge workers were already using AI in their roles. Most said it was helping them save time, focus on their most important work and be more creative. The concerning aspect, however, was that three-quarters of workers were using their own AI tools at work, without guidance or clearance from the top.

The other big risk of failing to adopt AI is being left behind. Gill says:

"There has to be broad acceptance that AI is now going to be widely incorporated into service delivery across industries. That is the emerging client expectation. Businesses have to be conscious that they will now be competing with rivals that have started with AI from the ground up and may be more digitally native and nimble."

AI adoption certainly does not come without complexity, but that is no reason to stay away. A thoughtful approach grounded in clear ethics, policies and principles has to be the way forward.

MANAGING TRANSFORMATIVE CHANGES THROUGH LEADERSHIP



We live in a world where change management is no longer associated with project implementation but is an important aspect of daily life. For business leaders dealing with economic uncertainty, geopolitical upheaval, supply chain threats and technological transformation, agility has become not a nice-to-have but an absolute prerequisite.

Another prerequisite that is too often overlooked in the C-suite job description, though, is empathetic leadership. To guide organisations through today's era of change, the tone from the top needs to be more than just confident, decisive and adaptable, it also needs to come with a heavy dose of empathy. Only then can leaders truly respond to the fast-moving needs of customers, employees, investors and other stakeholders.

Sahar Hashemi OBE, who founded Coffee Republic in 1995 and built it into one of the most recognisable high street brands, says times have changed and so has leadership.

"When I started building Coffee Republic, I was always told, 'Don't be so emotional – this isn't personal. It's business. Don't show any vulnerability',"

she says. "There weren't that many women around me, and I thought being businesslike meant putting on a corporate mask."

But, she adds: "I know the reason I took that company to 100 stores in five years was because I cared deeply: it was my resourcefulness, my problem-solving, and also my caring. Those qualities were my business superpowers."

Since Coffee Republic, Sahar has founded Skinny Candy, a brand of sugar-free sweets, as well as co-chairing the UK Government's Scale Up Taskforce and establishing Buy Women Built, a consumer movement to increase visibility of female founded brands.

"That softness is not a weakness," says Hashemi. "90% of women-built brands start from a personal need, solving a problem. Those founders have empathy with customers because they themselves are customers, and they have empathy with their teams because they lead in a different way. These women are redefining what leadership looks like – ultimately our customers are not AI, they are human beings, so we have to be out there listening to what they want."

Sara Bailey has been Senior Partner at Trowers & Hamlins since 2021, and says that, male or female, today it is critical to lead in an empathetic way.

"The leaders I find genuinely inspiring are those that actually care," she says. "They care about people and they care about clients."

Defining empathetic leadership

Bailey says an empathetic leader is someone who engages with people, listens and is authentic and true to themselves.

"It is also about humility," she says. "I don't think I know everything. Leadership is more about knowing yourself, knowing your weaknesses, and making sure you surround yourself with people that can help you address those weaknesses."

"A great leader is someone who makes others feel and look good, rather than themselves," continues Bailey. "It is someone who possesses emotional intelligence and can apply it when making business decisions. And it is someone who can step into the shoes of their employees, recognise their challenges and actively seek out ways to support them both personally and professionally."

Hashemi says:

"Leaders are always under pressure to know all the answers; to not ask stupid questions. But in a world that is changing so fast and shifting on its axis, clients need empathy and want to know you are listening. They want you seeing the challenges through their eyes, not your own."

Authenticity is also a key attribute of empathetic leaders. Bailey, who came to London from Yorkshire with a dream of becoming a lawyer but no family history in the profession, remembers being told to change in order to fit in. In fact, clients responded better when she brought her genuine self to work.

"I'm proud that one of the Trowers values is 'we're not afraid to be human'," she says. "Everyone is different and you don't have to pretend or try to be someone you're not."

Why now?

In the current climate, it has never been more important for business leaders to be fleet of foot, constantly listening and engaging with others to stay abreast of developments and adjust course when needed.

Technological transformation is a key driver of that need to be nimble. Bailey says:

“In the legal profession, we have to embrace AI, understand it and make it work for us. But it just brings everything up a level – a bot can do a lot of the work for us but clients are not robots and nothing can replace a trusted relationship when they are facing tough decisions. There is a new model forming, and relationships are at the heart of it.”

Empathy is not only vital to keeping up with customer demands, but also to attracting and retaining talented team members. The new generation of employees coming into the workforce is looking for more from an employer. Hashemi says:

“The younger generation are looking for purpose. That doesn’t mean that they have all got to be finding the cure for cancer, but they want to feel that what they are doing is having an impact. They are much more purpose-driven. By being close to customers, your people can feel they are solving real issues and making a difference.”

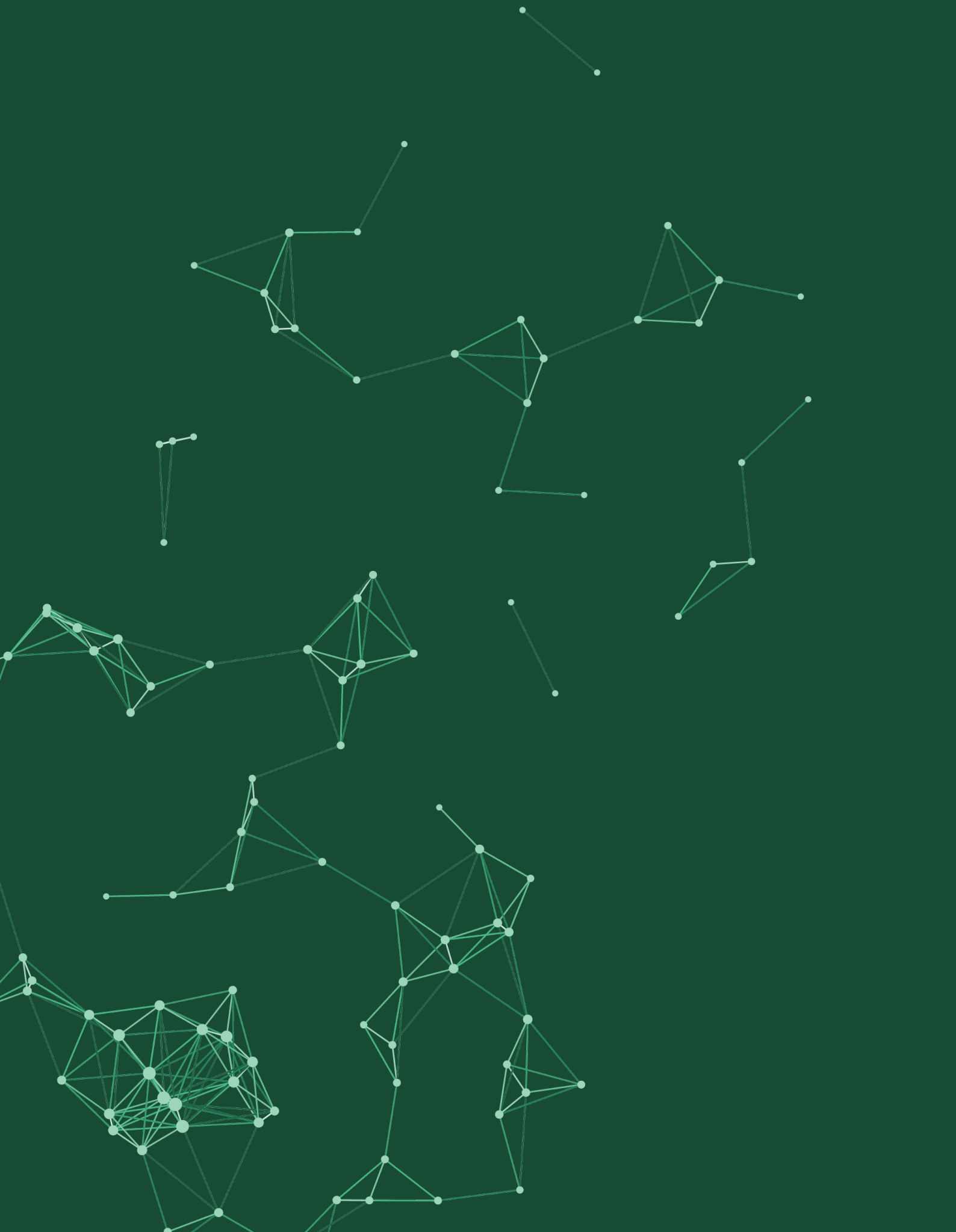
Leaders that invest time in getting to know individuals are better placed to embrace diversity of thought, diverse ways of working and new perspectives and approaches. We know that truly diverse workplaces breed innovation, healthy challenge and, in turn, higher productivity and better employee retention.

Bailey says: “Our most expensive commodity is our people and I don’t believe people come to work wanting to fail. Maybe some people don’t care, but they are the outliers. So as a leader, I have to ask myself how I can unlock every individual’s potential – that has to be the right business solution.”

An empathetic leader is not someone who is soft or weak, or someone incapable of making the tough calls. Instead, when they make business decisions, they really consider their impact and strive to make that impact positive.
Bailey concludes:

“Because empathy is viewed as soft, too often it is pushed down. But you can have great people skills and be a great leader. Someone who can inspire their people and build trust among their clients is going to succeed, even with all the challenges we face as leaders today.”

Making more time for human conversations may actually be the key to success in the new age of AI.



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.