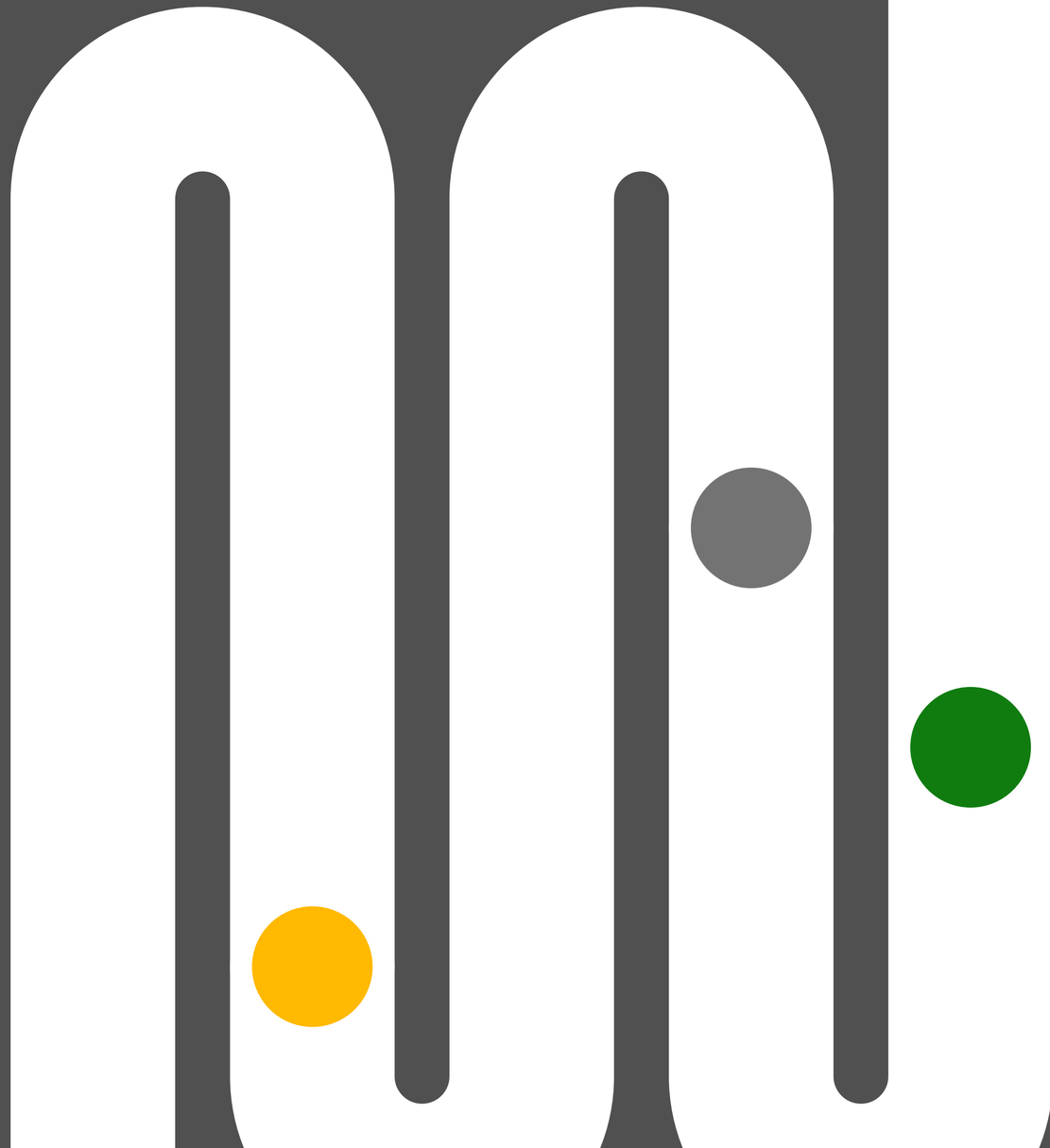
Microsoft Security

Mission Critical

Unlocking the UK AI Opportunity Through Cybersecurity

Click here to get started



Cybersecurity In The Era Of AI

There is much excitement around AI and it's dominating conversations in boardrooms, newsrooms and everywhere in between. It truly is the defining technology of our time. Generative AI is transforming how organisations operate. They are using it to increase productivity, save time and boost creativity, which in turn means they can serve their customers better, bring new products to market faster and use it to train their people. So, when I think about advances in AI in the context of the UK, a country that has always been quick to embrace technology's potential, the opportunities seem endless. Yet, to fully realise the benefits of generative AI, we must trust it: trust that it prioritises safety, privacy and security. We can only build a prosperous future if we start from secure foundations.

Our mission at Microsoft is to empower every person and every organisation on the planet to achieve more. In the era of AI, that means using technology to unlock possibilities: for people, for industry and for society more broadly.
And it also means building, deploying and using it safely and responsibly. We are deeply committed to advancing AI in a way that is trustworthy and beneficial for all.

The UK government is keen to build trust in emerging technologies too, taking a leadership position in terms of AI safety and regulation. The Bletchley Declaration, signed by 28 countries attending the AI Safety Summit in late 2023, enables global cooperation on AI safety and recognises the known, and unknown, risks emerging technologies represent. And these risks include cyberattacks.

Because just as businesses and governments are keen to tap into AI's potential, so are bad actors. Traditional add-on security solutions can no longer keep pace with the threat posed by cybercriminals, meaning British organisations must be ready to fight fire with fire. Unless we arm ourselves with AI-enabled cyber defences that are stronger than AI-enabled cyber threats, it will be difficult, impossible even, for us to grow and, ultimately, thrive as a nation.

Doing so requires investment. Microsoft is playing its part: in late 2023 we announced a landmark £2.5bn investment in data centres, AI skills and security in the UK, our biggest investment in our more than 40-year history in the country. But cybersecurity is a team sport. As this report explains, there is vital work required of all of us, if the UK is to stay cyber secure in the era of AI.

> We can only build a prosperous future if we start from secure foundations

Indeed, using a new cybersecurity model created by independent researchers from Goldsmiths, University of London, we find that only a handful of British organisations are currently resilient to evolving cybersecurity threats. Others find themselves at serious risk of falling victim to attacks. This lack of resilience is holding back innovation, which in turn, holds back growth.

It's not all bad news, though. The same research model shows that organisations using AI are twice as resilient to cyberattacks as those that are not. I know from my conversations with business and government leaders across the UK, that they are keen to use AI to help bolster their defence against cyberattacks. Doing so will not only help their operations, but also help attract future investment. And in turn, help the UK fulfil its ambition to become the most secure place to live and work.

This report explains how the UK can live up to its potential. It sets out five ways the country can become a cybersecurity superpower and five steps business leaders can take to boost their organisation's resilience. This is a report about action. And about opportunity. But above all, it's about leadership. And how the UK can be a global cybersecurity leader in the era of AI.

Clare Barclay
CEO, Microsoft UK

Chapter 1

State of revolution

"Artificial Intelligence (AI) presents enormous global opportunities: it has the potential to transform and enhance human wellbeing, peace and prosperity."

So begins the landmark Bletchley Declaration signed by 28 countries attending the AI Safety Summit in Britain last November.

It is a familiar and entirely accurate refrain. From chatbots to voice assistants, large language models to self-driving cars, the sheer speed and scale of AI's evolution is sparking a revolution in government, business and the lives of citizens all over the world.

In the UK, there is a clear ambition to be at the forefront of this change. The National AI Strategy sets out a 10-year plan to turn the country into a "global AI superpower" through a combination of strategic investment, wide-ranging innovation, support and responsible governance.

The Bletchley Declaration places Britain at the heart of an international agreement to drive safe and effective AI deployment worldwide. Likewise, initiatives such as The Artificial Intelligence for Decarbonisation's Virtual Centre of Excellence (ADViCE) and the Turing AI Fellowships, which is designed to attract, retain and develop top AI talent, underline the UK's pioneering aspirations.

Maintaining momentum

As the UK government has recognised - to lead in AI, we must first be able to trust the technology. Principles of privacy, safety, accuracy and security are central to the Bletchley Declaration.

Secure foundations will be critical for AI systems, yet a new study commissioned by Microsoft reveals that cyberattacks could be costing UK organisations more than £87 billion each year.

Our study, conducted by independent researchers from Goldsmiths, University of London, spoke to more than 1,000 senior decision-makers and senior cybersecurity professionals across a variety of private and public sector organisations (more than 650 of which work within large organisations), as well as more than 1,000 employees.

It found that the majority of decision-makers (52%) and senior security professionals (60%) fear that current geopolitical tensions will increase cyber risks to their organisation.

Consequently, more than half (55%) see a lack of robust protection as a threat to the UK's economic growth while two-thirds (69%) recognise that Britain will need stronger cybersecurity defences if it is to achieve its goal of international AI leadership.

Encouragingly, Britain is already leading the international field in cybersecurity. The country was ranked fourth in the National Cyber Power Index in 2022 (extending a long period in the top 10) and second in the Global Security Index. Building on this momentum will be crucial as the threat landscape evolves.

Leading the world on secure AI

"The advancement of AI has rapidly accelerated in recent years, infiltrating every sector and fundamentally reshaping business operations and decision-making processes. However, this swift technological progress also brings forth new challenges and threats. A plethora of cybersecurity risks and vulnerabilities have surfaced in this domain, many of which remain only partially understood.

Organisations and policymakers find themselves confronted with the formidable task of harnessing AI's transformative potential while simultaneously navigating an ever-evolving threat landscape. Ensuring the well-being of people, processes, and technology in an AI-augmented world demands unwavering vigilance and a commitment to forward-thinking strategies that necessitate continuous adaptation.

The UK stands at a pivotal juncture. The UK has led the world in cybersecurity strategy and policy, and the cybersecurity sector has demonstrated remarkable growth, resilience, and expertise. With world-leading cyber firms located here, the UK possesses exceptional pipelines for talent and investment. Having been leader in cybersecurity there is now a unique opportunity for the United Kingdom to continue that role in the adoption of AI. We can build on our reputation as a centre of excellence for cybersecurity to lead the world on secure AI."

Siân John
Chief Technology Officer
NCC Group

A changing game

The need to safeguard vital information infrastructure from bad actors has long been key to everything from the performance of British businesses (and, by proxy, the UK economy) to the safety and prosperity of citizens, but AI is unquestionably changing and intensifying the game.

From enhanced phishing attacks to polymorphic malware, cloning and imitation to the exploitation of prompt interfaces, cyber criminals now have the tools and capabilities to become ever more sophisticated, nuanced and networked in their attacks. As David Wakeling, Partner, Head of Markets Innovation Group (MIG) at international law firm Allen & Overy, says: "Data leakage is a serious threat that must be averted at all costs."

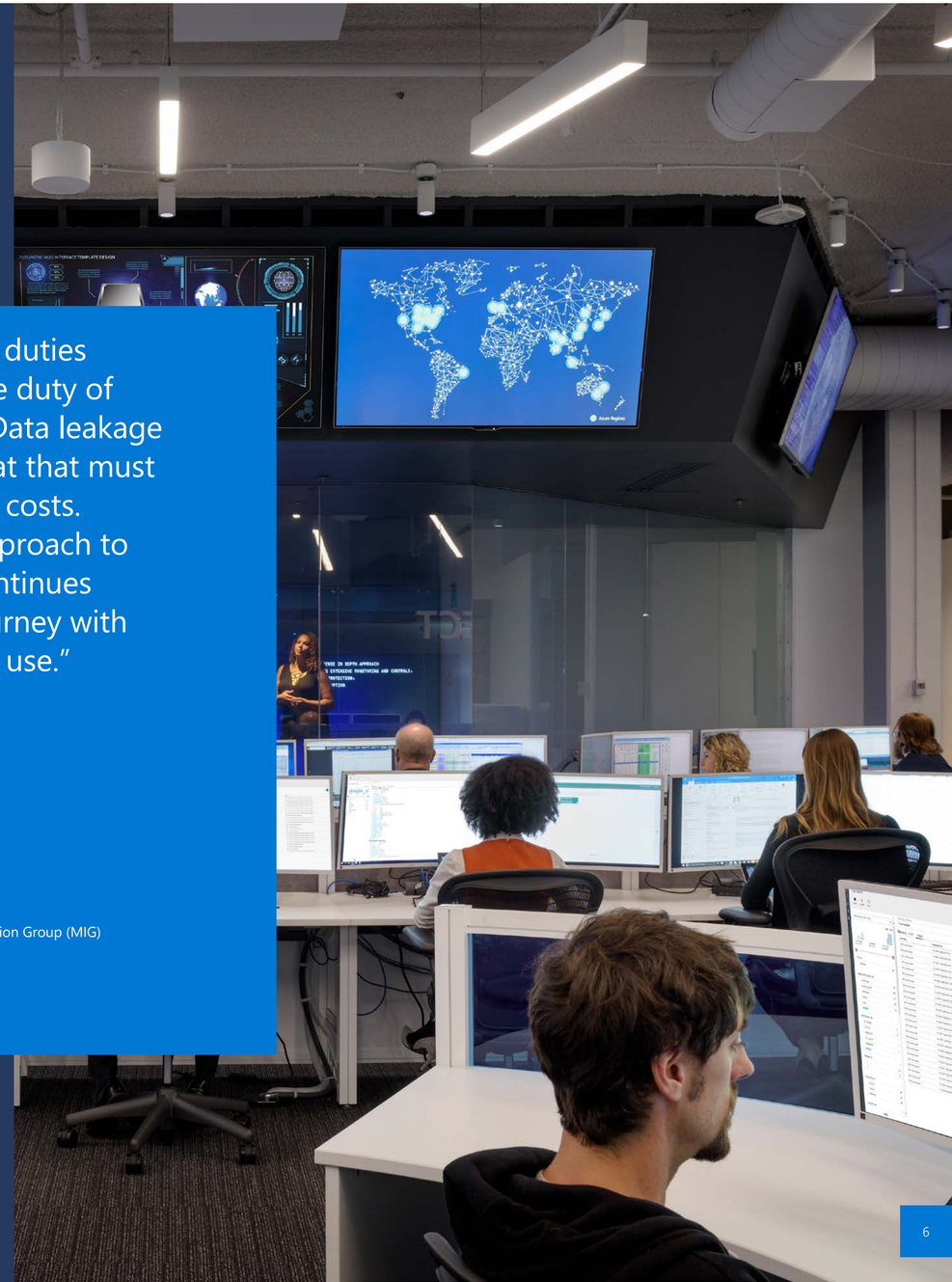
As we will see in this report, there is more that UK organisations can do to build cyber resilience and help the UK to get ahead of the AI curve.

Too many organisational leaders express concerns in an absence of up-to-date cybersecurity skills and knowledge within their workforce. Many also cite limited financial capital allocated to protecting against attacks while others report insufficient investment in research and innovation, be that in updating existing systems or in adding new lines of defence.

Each of these challenges must be addressed—and quickly.

> "One of the first duties of a lawyer is the duty of confidentiality. Data leakage is a serious threat that must be averted at all costs. This rigorous approach to data security continues to shape our journey with every AI tool we use."

David Wakeling
Partner, Head of Markets Innovation Group (MIG)
Allen & Overy



Fighting fire with fire

As for how, Paul Kelly, Director of the Security Business Group at Microsoft UK, says it all comes down to fighting fire with fire. "Just as AI is enabling cyber criminals to be more stealthy, sophisticated and well-resourced in their attacks, AI-based tools can help leaders better secure their organisation and tip the balance back in their favour," he explains.

In other words, to become an AI superpower, the UK must cement its position as a *cybersecurity* superpower too.

This will require more than investment in the right AI technologies and solutions. The UK must also act to foster the necessary skills and capabilities within the workforce. To boost spending on R&D and innovation. And to create education programmes that help citizens overcome concerns about AI and cybersecurity to play their part in the journey ahead.

The government's recently announced £114 million increase in funding for the National Cyber Programme, accompanied by enhanced spending on critical cyber skills training, infrastructure, research and development, innovation, defence and intelligence, was therefore a welcome statement of intent.

Superpowers secured

While the resources required for this national cybersecurity transformation are considerable, so too could be the rewards. First and foremost, the rapid adoption of AI-enabled defences will help protect UK organisations against the financial, operational and reputational costs of successful attacks. It will also help build the country's reputation as a hub for AI innovation, sending a clear message that Britain is a safe place to do business.

But more than that, AI-based cybersecurity is already a lucrative and growing sector in its own right, with recent figures suggesting the global market will surge to around $135 billion by 2030, compared to just $15 billion in 2021.

This provides an exciting opportunity for UK organisations to unlock new sources of revenue, drive international growth and attract industry-leading talent.

To become an AI superpower, the UK must cement its position as a *cybersecurity* superpower too

In this report, we consider how UK organisations are faring on their journey to AI leadership. We discuss the importance of developing AI-enabled defences strong enough to deal with AI-enabled threats. And we set out a five-step blueprint for how the UK can cement its pre-eminent position on the global stage and how leaders can support this mission by boosting their own organisation's cybersecurity.

However, we begin in the next chapter by exploring the nature of the AI opportunity for British businesses along with the far-reaching benefits available to those who step up and lead. In a future built on AI, the UK has its sights firmly set on superpower status. Now is the time to secure this.

Putting cybersecurity front of mind

The whole field of artificial intelligence is rapidly developing – and it's gripping the public's imagination at the same pace. While this new way of living and working offers many opportunities, it brings with it many challenges – not least for British businesses.

As the UK's national technical authority, we know AI has the potential to improve cybersecurity by dramatically increasing the accuracy of threat detection and response. But, as highlighted by Microsoft in this report, it must be underpinned by secure foundations.

We are committed to working in partnership with UK industry, as well as our international counterparts, to realise the benefits provided by AI and ML systems.

And we continue to work in close collaboration with those partners to ensure our guidance keeps pace with the development of AI technologies, including for non-technical audiences.

The first major global summit on AI Safety led by the UK Government at Bletchley Park last November was an important moment for the global technology community to set its intentions to make AI work for our people, our businesses and our societies.

For businesses, this means putting cybersecurity front of mind. We offer a suite of services to help organisations of all sizes do just that – ranging from published guidance; to online tools; to the Cyber Essentials scheme, which helps protect organisations of all sizes against the most common cyber attacks.

While we continue working with industry to keep pace with AI developments, we welcome Microsoft's report for highlighting the need to build organisational resilience across the UK at a rate never known before.

Jonathon Ellison
Director for National Resilience and Future Technology
The National Cybersecurity Centre

Chapter 2

The AI effect and opportunity

$135 billion by 2030. That, as we saw in the previous chapter, is the predicted size of the global AI cybersecurity market by 2030.

With a strong heritage and reputation in the field, UK organisations have a real and compelling opportunity to seize a significant share of that figure.

Given the leadership position the government has already taken on international AI governance, it is clear the nation's policymakers are well aware of this opportunity. It is now up to businesses to follow suit.

Indeed, our study finds only 27% of UK organisations currently use AI specifically to strengthen their cyber defences. Or put another way, almost three-quarters (73%) are failing to deploy the most extensive and robust form of cyber defence. This carries a double danger: being more exposed to attack and missing out on the AI opportunity at hand.

What is AI-enabled cybersecurity?

"AI for cybersecurity uses AI to analyse and correlate cyberthreat data across multiple sources, turning it into clear and actionable insights. Security professionals can then use these insights for further investigation, response and reporting. If a cyberattack meets certain criteria defined by an organisation's security team, AI can also automate the response and isolate the affected assets. Generative AI takes this one step further by producing original natural language text, images and other content based on patterns in existing data."

Paul Kelly
Director – Security Business Group
Microsoft UK

The AI effect on cybersecurity is especially visible when it comes to the resiliency of organisations to attack.

The researchers' analysis shows that those organisations using AI in cyber defence could withstand 254 successful attacks on average before the equivalent of their annual revenue is wiped out. However, this drops to just 106 attacks of the average organisation not deploying AI in this manner. In short, organisations using AI in cyber defence are more than twice as resilient to cyberattacks.

These organisations are also likely to suffer 20% fewer costs when successfully attacked. The average cost of these attacks across businesses of all sizes was £20,700 (£148,700 for large organisations), slightly higher than the £15,300 featured in the Government's UK Cybersecurity Breaches Survey 2023. But for organisations deploying AI-enabled cybersecurity, this average cost dropped to £16,600, or 20% fewer costs, as they are able to detect and respond to the attack more quickly.

Extrapolated across the entire business community, the impact is significant.

> Organisations that use AI-enabled cybersecurity are twice as resilient to attacks as those that do not and suffer 20% less costs when attacked.

As we have seen, the research estimates the current cost of successful cyberattacks to the UK economy to be at least £87 billion. Through the widespread adoption of AI-enabled cybersecurity systems, organisations could collectively save the national economy as much as £52 billion every year. All while further underlining the security of the UK's trading landscape.

Beyond the bottom line

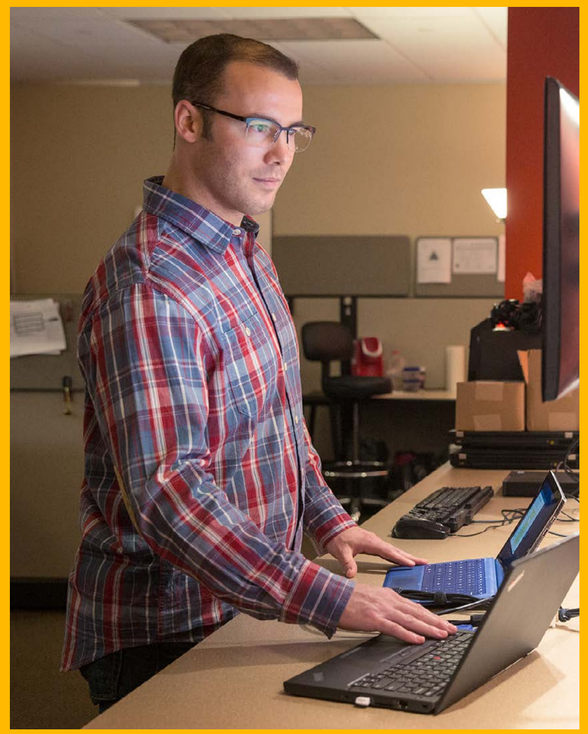
Alongside the financial opportunity, the adoption of AI-enabled defences can support the UK's leadership in a range of other ways too. For example, by taking on more labour-intensive and time-consuming security functions, AI can help alleviate skills gaps and talent shortages—welcome news for the 69% of business leaders who are unsure or do not find it easy to hire employees with cybersecurity expertise.

Additionally, it can provide opportunities to elevate existing staff's capabilities and education through personalised learning, on-demand training, skills augmentation and data driven insights. All while attracting a new generation of talent who want to work at the cutting-edge of AI innovation. It even offers the potential to solve complex challenges around data quality assurance, enriching and prioritising alerts, managing security posture analysis and internal communications—all of which will be vital to success in an increasingly dynamic and digitised operating landscape.

See **Risk and Reward** to discover how international law firm Allen & Overy is using AI to address security risks while enhancing the performance and productivity of its people.

In other words, there is far greater motivation for organisations to adopt AI-enabled cybersecurity than simply financial return or threat mitigation. So much so argues Prof. Hoda Al-Khzaimi, Director, EMARATSEC Center for Emerging Tech and Advanced Research Acceleration in Security, AI and Cryptology, that it is time for UK organisations to embrace a new era of "resiliency by design" in which emerging and critical technologies as in AI and cybersecurity progress go hand in hand to reach new ecosystem and industrial impact.

As she explains: "Resiliency by design means that we don't have to micromanage security. It is the ability of a hardware or software to go back into a status of security even when it has been pushed into a security degradation situation. Having that adaptive behaviour means that if we are building a cybersecurity framework that goes hand in hand with AI, it's not just to fill the innovation curve, it's to expand it to a new horizon that did not exist in the past."



Lifting the burden on security teams

"A common trend we see is that knowledge of organisations' systems and networks is concentrated in a small number of people, which puts a lot of pressure on those same people when there's an incident. Also, when these key team members leave the business, the knowledge and detailed insights they have often leave with them.

Another issue is ensuring the optimal configuration of security alerts. While alerting on anomalous activity is crucial, if too many alerts are let through, it increases the pressure on security teams given the number of false positives they have to contend with. Instead of having the space to identify anomalies, which could be the sign of a legitimate security issue, the focus sometimes shifts to closing tickets, which ticks a box, but isn't optimal from a security posture perspective.

Even if a company has secured its own business, there's also the risk of supply chain incidents to be mindful of. The effects of a cyber incident can be spread globally across many interlinked organisations, and the associated regulatory implications and remedial work can be difficult and time consuming.

AI will have an increasing role in addressing these issues. It can be used to lift the burden on small security teams that feel stretched. The more repetitive tasks that can be automated, the more space teams have to breathe, observe, and think through security issues thoroughly. AI driven insights can be shared in plain English throughout the business to everyone who needs it – including senior leadership, so security becomes a shared responsibility, rather than being concentrated within IT and infosec departments.

If a security breach takes place, AI can potentially be leveraged to identify all obligations to inform relevant stakeholders and help automate the process. For large organisations with hundreds of commercial counterparties, this can save huge amounts of time and resources."

Ffion Flockhart
Global Head of Cybersecurity
Allen & Overy

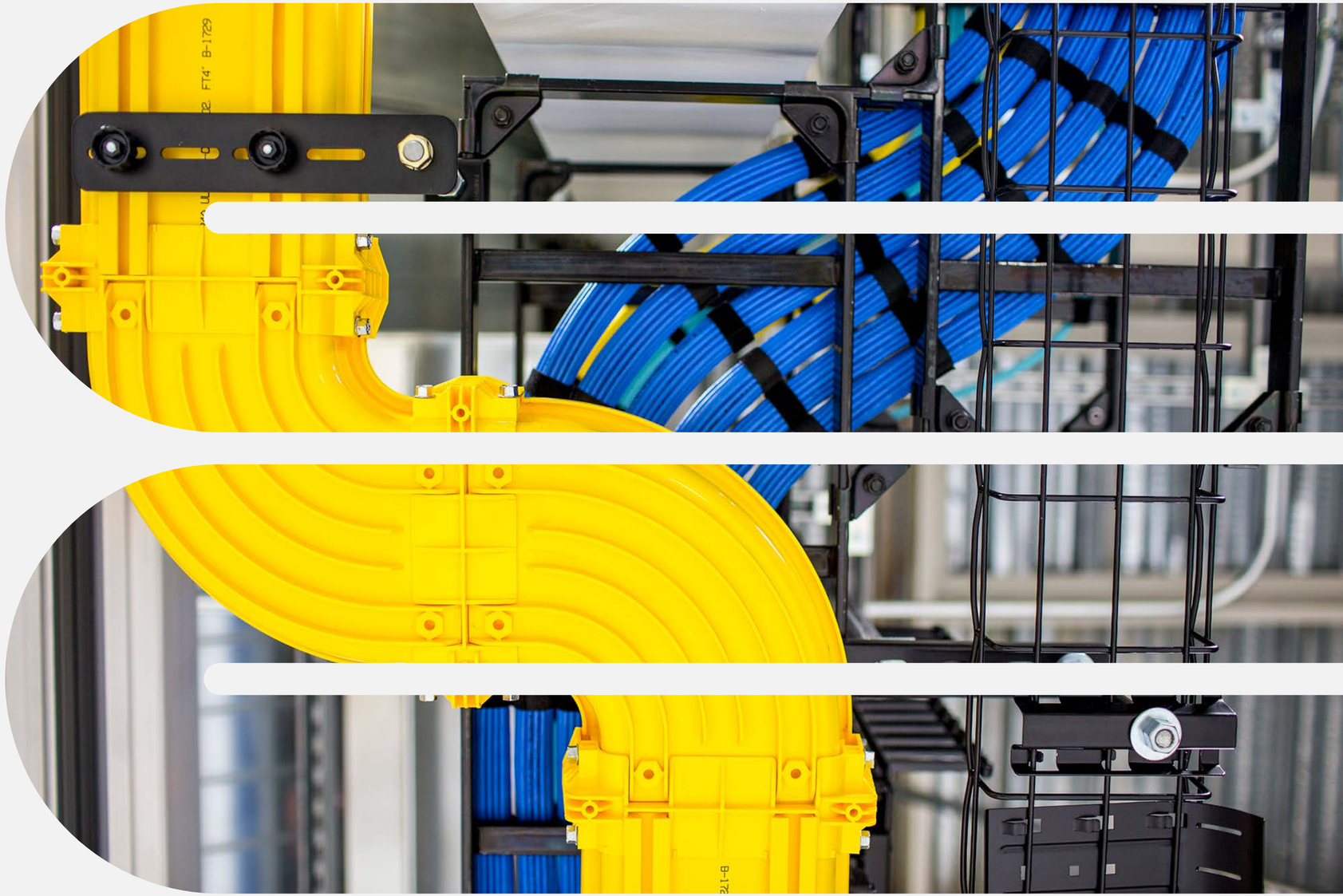
Race to resilience

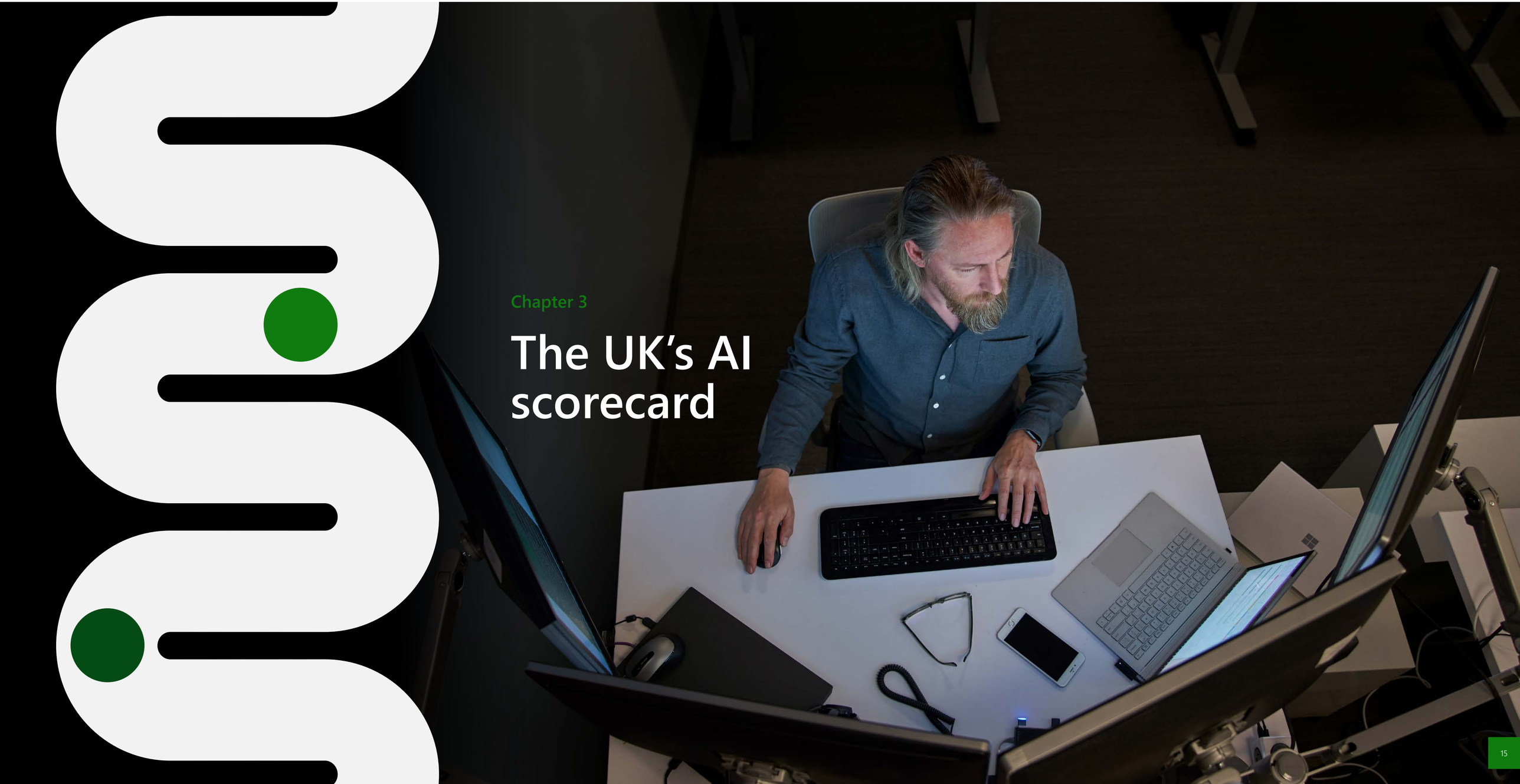
To reach this point, business leaders must first understand where they are now. Using a specially created academic model centred around six key behaviours and capabilities, Goldsmiths researchers have precisely assessed the success of UK organisations in establishing and executing an effective, long-term cybersecurity strategy.

These six dimensions, which mirror the set of behaviours and capabilities that are core to other international indices, provide the building blocks upon which strong and efficient cybersecurity is built. Yet, our study reveals only a small minority of UK organisations are currently in a position to consider themselves resilient to AI's shifting threat.

So, what marks these organisations out from the crowd? Where and why are the others vulnerable? And what can business leaders do to achieve true resilience by design and, in doing so, play their part in powering the UK towards its global superpower ambitions?

Answering these questions is at the heart of benefitting from the AI effect and seizing the AI opportunity. We address them directly in the remaining chapters of this report.





Chapter 3

The UK's AI scorecard

As we saw during Chapter 2, an effective AI-enabled cybersecurity strategy could double the resiliency of UK organisations to cyberattacks and cut the costs of successful attacks by 20%.

Both individually and collectively, this offers a compelling opportunity to gain a competitive edge.

Yet, there is a danger this opportunity could pass unseized. Just 21% of respondents to our study currently deploy AI in the detection of cyber vulnerabilities while only 27% are using it specifically to strengthen their cyber defences.

In some cases, the problem comes down to a lack of awareness around the challenge at hand. For example, over a quarter (27%) of UK decision-makers have no idea of the cost to their organisation of a successful cyberattack. More than half (53%) do not know how long it takes to recover from one.

As you might expect, understanding of these issues is much greater among security professionals. But the point is clear: to become resilient by design, responsibility for cyber risk mitigation and response must move beyond the IT department to permeate the mindset and operations of the entire organisation.

This integrated approach is a central pillar of any effective cybersecurity strategy. As Prof. Hoda Al-Khzaimi, Director, EMARATSEC Center for Emerging Tech and Advanced Research Acceleration in Security, AI and Cryptology says: "We still don't evaluate cyber risks correctly in 2024. They are prime corporate assets and need to be included within organisations' valuation model to make sure they are coupled tightly with any kind of decision they make."

Of course, these cyber risks can take many forms. And interestingly, as shown in **Figure 1**, many of the dangers that keep senior security professionals up at night, including malware, phishing and password leaks, could be considered more 'traditional' than some of the latest AI-enabled threats. And while decision-makers and senior security professionals are largely aligned in their concerns, there is a notable difference of opinion when it comes to IoT risks (38% of senior security professionals worry about this compared to 12% of decision-makers).

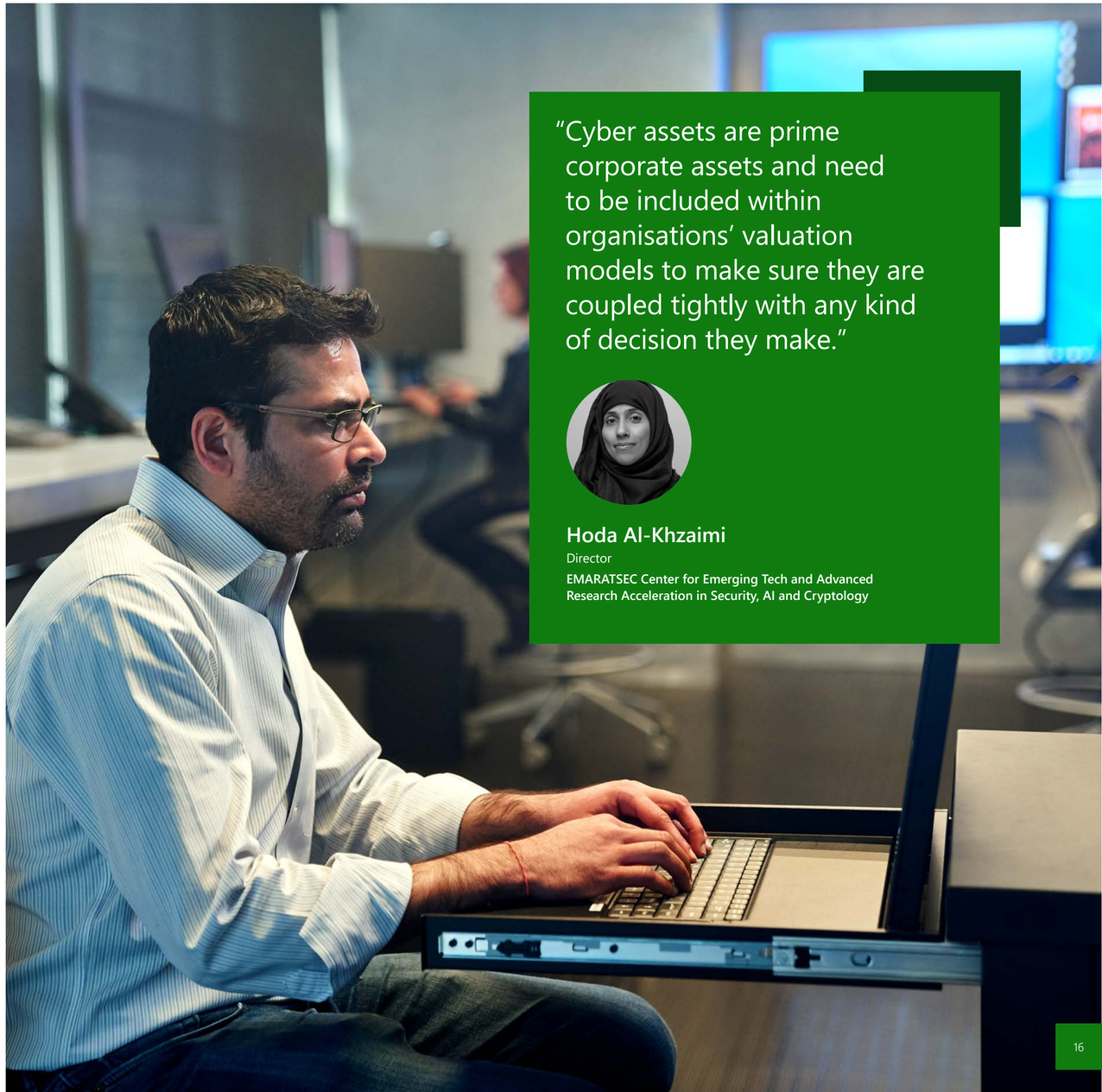
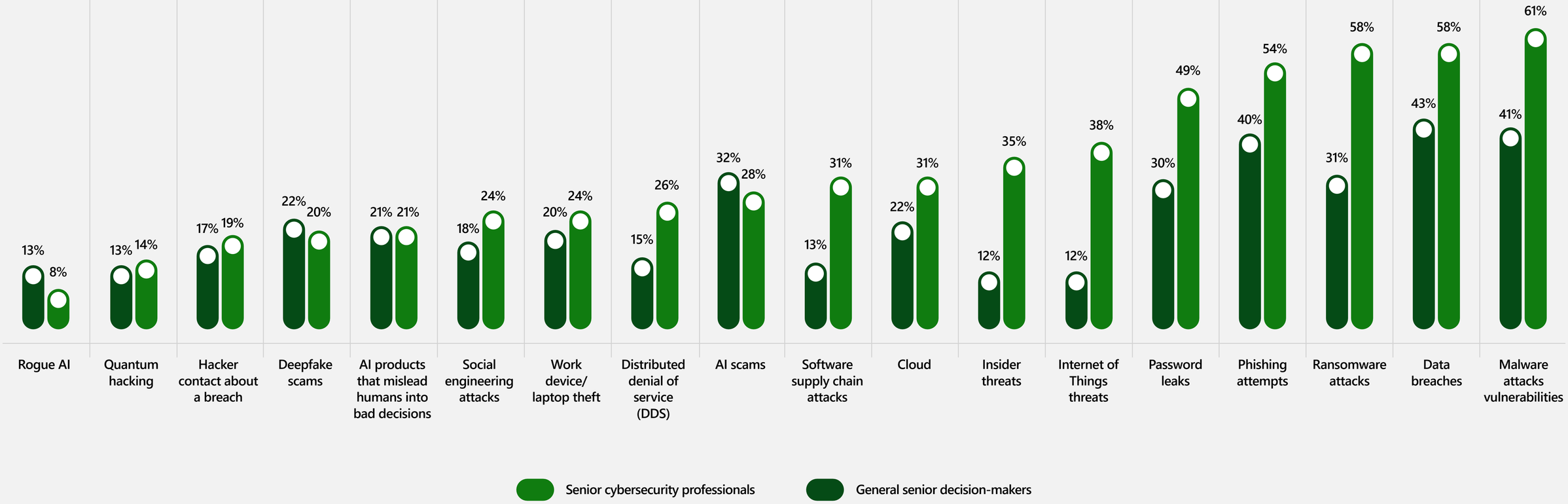


Figure 1
Security professionals' top cyber concerns



A model of success

However, what is true across the board is that AI-powered solutions provide the most effective line of defence. And by using the new model created by Goldsmith's researchers, it is possible to evaluate exactly where different UK organisations are along their journey to deploying them.

The model assesses six key dimensions of cybersecurity—three capabilities and three behaviours—which, together, provide the bedrock of a robust and effective strategy for prevention, detection and response to attacks. **See Figure 2.**

Figure 2
The six dimensions of effective AI defence

These dimensions are:

Capabilities

The systems, processes and tools that determine an organisation's ability to safeguard itself against cyberattacks.

1. **Resources:** having access to talent with cybersecurity skills and a dedicated budget for protection against cyber threats and their impact.
2. **Agility, AI and automation:** cyber threats become more sophisticated with AI, so operations, including cybersecurity, must become more resilient too. In a more agile and responsive organisation, AI is key to most processes.
3. **R&D and innovation:** due to shifting threats and constant technological advances, legacy systems are often easily penetrable, so must be regularly updated. For most businesses, this means investing in innovative AI-enabled solutions from external partners.

Behaviours

The technology culture of an organisation, indicating how familiar it is with proper governance and its openness to new ways of managing cybersecurity.

4. **Transparency and technical knowledge:** establishing and enforcing rigorous, organisation-wide policies for the responsible and ethical use of AI as well as a culture of knowledge sharing.
5. **Organisational buy-in:** a leadership approach that champions best practice in cybersecurity while equipping and empowering employees at all levels of the organisation to take part in the journey.
6. **Trust and mindset:** when both internal and external stakeholders have confidence that the organisation is doing the right things to remain protected, it leads to higher trust, better decision-making and better preparedness.

Could do better

The model sheds fascinating light on the UK's cybersecurity landscape. For example, when it comes to capabilities, fewer than half (49%) of leaders claim to understand the cybersecurity skills their workforce requires and only 56% have offered training to improve their staff's understanding of best practices.

Many decision-makers (49%) and senior security professionals (70%) fear the increased use of AI poses risks to their organisation too. Yet, at the same time, fewer than three in five organisations (55%) are prepared for cyber threats and just 43% have designated resources for cybersecurity-related events. Here there are considerable disparities between industries too, with tech companies (70%) and financial institutions (65%) far ahead of retailers (26%) and education (29%).

As for the behavioural elements of the model, again we find work to be done. Transparency remains an issue with only 15% of organisations willing to share information about incidents with customers, even though it is they who often ultimately bear the cost. Almost one in five organisations (19%) admit they do not share information about cyber incidents and risks with customers at all.

> Only 13% of UK organisations are currently classed as resilient to cyber threats

In line with the UK's leading position on governance, issues of ethics, privacy and security are also the top concerns among business leaders regarding the increased use of AI. Yet, often, this is without any serious internal framework of regulation and accountability to address them. And while 55% of senior decision-makers agree cybersecurity is a business priority in their organisation, 30% also believe this makes them less agile.

Encouragingly, however, governance is stronger in organisations that employ senior security professionals, improving everything from the roll-out of cybersecurity policies to the monitoring of risk, both within their own operations and across their supply chain. This further emphasises the importance of having the right people and expertise in place.

Classified information

So, what does all this mean when it comes to the cybersecurity performance of UK organisations? Based on the parameters of the model, we are able to group them into three broad classifications:

Resilient – those that are secure by design, following international standards for protecting their business, customers, staff and investors. Crucially, they are on the front foot when it comes to cybersecurity, adopting AI in their businesses and using it to detect and respond faster to threats. Just 13% of UK organisations currently fall into this category.

Vulnerable – these organisations have defensive systems and processes in place but require additional investment and support to accelerate their journey towards resilience. Some are adopting AI in their business operations but only a few are using it in the detection and mitigation of risk. This is the most common category, featuring 48% of UK organisations.

At High Risk – here we find those that have still not got to grips with the importance of cybersecurity. Held back by uncertainty, scepticism and fear, this group is not deploying AI for risk detection while most fail to use sophisticated AI in their general business at all. Of the UK organisations surveyed, 39% fall into this category.

See **Figure 3** for more details around the specific characteristics of organisations in each category, along with the impact this has on their business preparedness, performance and continuity.

Figure 3
Classifying UK organisations' cybersecurity performance

13% Resilient

- Cybersecurity is a business priority and embedded in business strategy
- Regular assessment of vulnerabilities allows quick response to threats
- Business continuity plans include recovery strategy
- Transparent with all stakeholders about cybersecurity risks and events, including employees, vendors, investors, clients and government
- Have a strong commitment to investment in innovative technologies and invest well above the national average in R&D and innovation
- Confident they know the skills they need to hire for cybersecurity roles
- Trusted by the public and their employees to do the right thing

48% Vulnerable

- Cybersecurity is considered as a business priority by only a small number of leaders
- Regularly assess vulnerabilities but lack the proactive detection and prevention approach of Resilient organisations
- Inconsistent in response times to attacks and less likely to have business continuity plans
- Leadership and employees are informed about any cyber threats but not all stakeholders are notified
- More likely to be lacking in-house cybersecurity skills than Resilient organisations
- Invest in new technologies but not enough to keep pace with the rate of innovation and change

39% At High Risk

- Leadership are not regularly informed about cyber threats leading to a lack of leadership engagement when attacked
- Unlikely to have a business continuity plan, making them slow to respond to attacks
- Limited ability for risk mitigation as they are less likely to regularly monitor and assess vulnerabilities across their operations
- Do not have a dedicated budget for upgrading cybersecurity or to cover cybersecurity costs
- Find it difficult to assess what talent is required within their workforce, impacting recruitment and training
- Low investment in technological upgrades and skills programmes

Positive progress

Naturally, the fact that so few UK organisations are considered resilient to the cyber threat landscape is cause for concern—both for their own security and for the stymying effect it could have on the UK's broader ambitions for AI leadership.

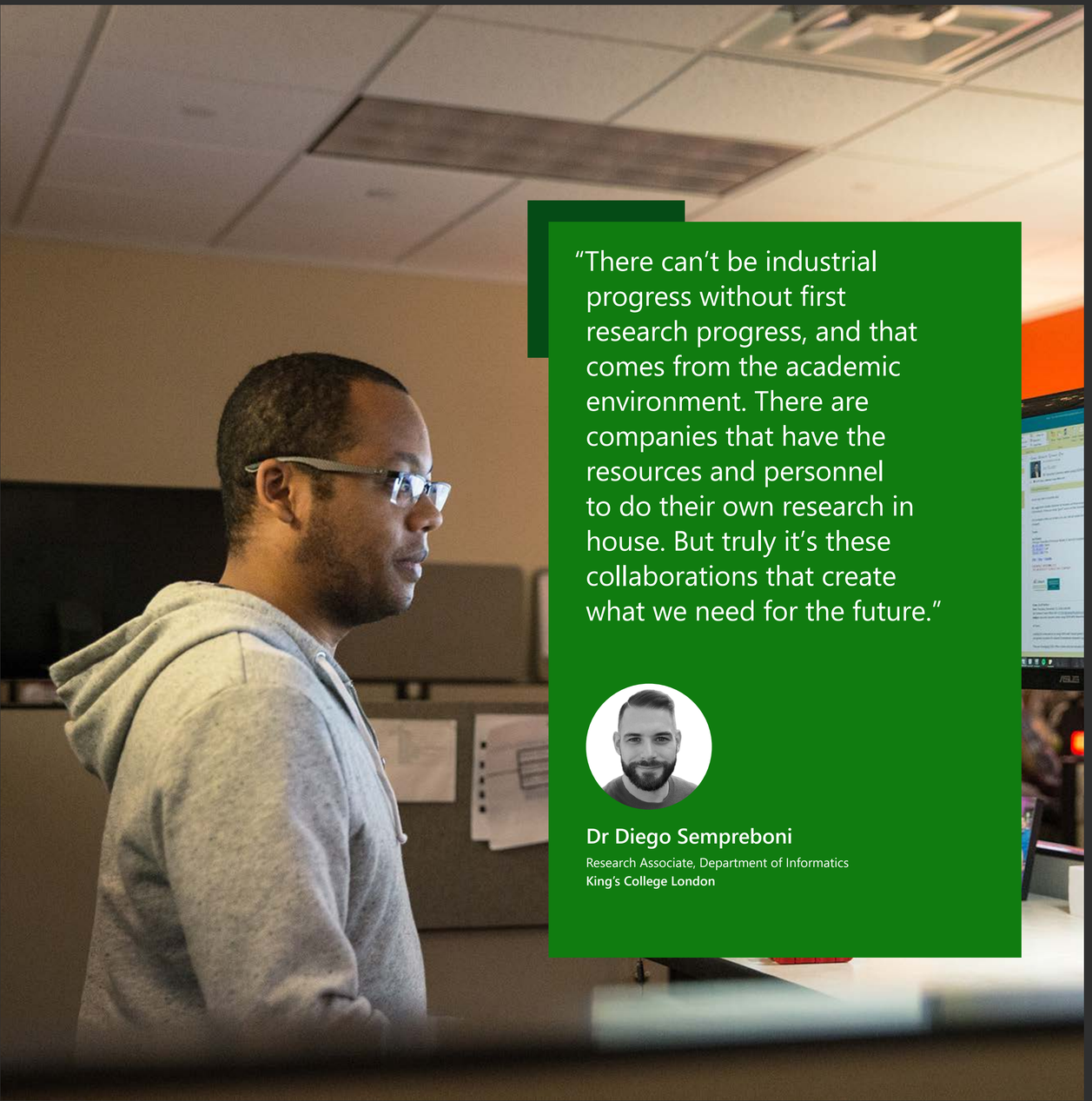
Recent figures show that if cybercrime were measured as a country, it would be the world's third largest economy, with its associated costs expected to reach $10.5 trillion (£8.4 trillion) annually by 2025. Likewise, the Bletchley Declaration warns "there is potential for serious, even catastrophic, harm, either deliberate or unintentional, stemming from the most significant capabilities of these AI models."

Those UK organisations classed as Vulnerable and/or At High Risk therefore face the very real prospect of falling victim to sophisticated cyberattacks, be that in the short-, medium- or long-term. Even the 13% currently deemed Resilient must continue to invest in renewing and updating their systems to counter continuously shifting threats. Yet concern need not equal despair; there is much reason for positivity too. The UK is one of the first governments globally to publish a National AI Strategy, offering a valuable platform of support and guidance for organisations looking to arm themselves against attacks. Partnerships with academia also offer a powerful path to progress, particularly for those businesses without the resources to conduct their own AI innovation programmes in-house.

"AI has become a critical component in cybersecurity—a foundation for resilience. As the threat landscape evolves rapidly, AI has and will continue to play an important role in the detection and management of risk both in the defensive and offensive realms.

But synergy between humans and AI is key—if you do not have human resources to multiply the effectiveness of AI, you will get no result. History shows us that technological advancement is a multiplying factor, we cannot afford to ignore the potential value AI offers our industry."

Steve McKeaveney
Head of Customer Success
ITC Secure



"There can't be industrial progress without first research progress, and that comes from the academic environment. There are companies that have the resources and personnel to do their own research in house. But truly it's these collaborations that create what we need for the future."

Dr Diego Sempreboni
Research Associate, Department of Informatics
King's College London

It is also important to note that the 48% of organisations classified as Vulnerable are, at least, getting some things right.

This puts them on the right path to resilience and, when allied to the 13% that are already there, means that nearly two-thirds (61%) of British businesses have the awareness and willingness to achieve their cybersecurity objectives.

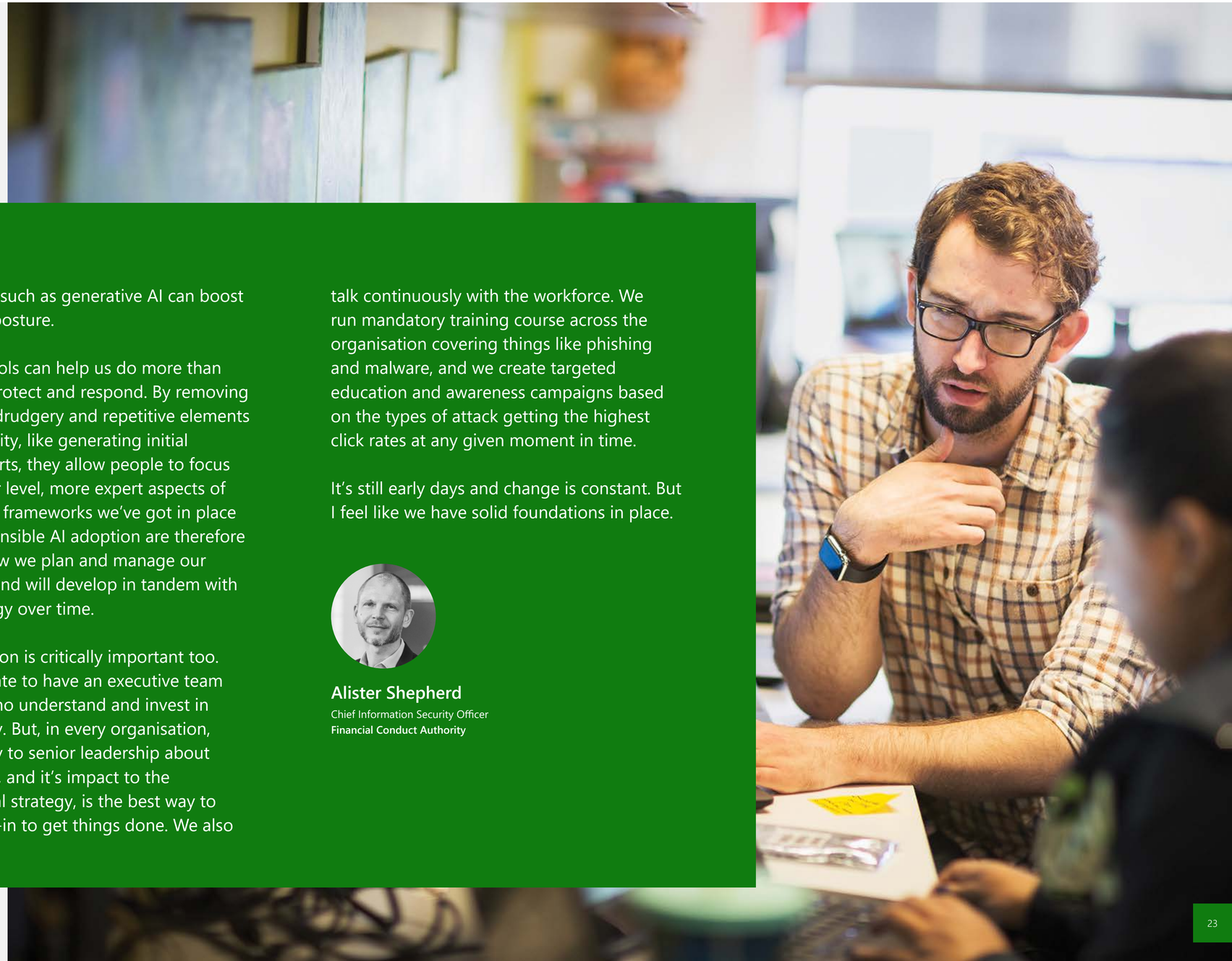
Most positively of all, there are immediate steps organisations in every classification can take to bolster and extend their cybersecurity using AI and, in doing so, support the UK's vision of international leadership.

Some of these actions must be taken individually, helping At High Risk organisations improve to become Vulnerable and Vulnerable organisations progress to Resilient.

Others fall within the collective remit of the government and business community, spanning everything from cross-industry knowledge sharing and talent programmes to targeted investment and a more coherent and cohesive regulatory framework. Regardless, the need for action at both an organisational and national level is clear—and urgent. If the UK is to secure its position as an international AI frontrunner, it must be just as ambitious and expansive about its cybersecurity capabilities too.

In the following chapters of this report, we lay out a blueprint for doing exactly that.

If the UK is to secure its position as an international AI leader, it must be just as ambitious and expansive about its cybersecurity capabilities too.



The case for the defence

The FCA processes data relating to around 45,000 UK financial services organisations, many of which are priority targets for malicious actors. We must therefore safeguard our own systems and data against any cyberthreats we could be exposed to as a result.

This task is getting more nuanced and challenging. Geopolitical issues, particularly around Russia and the Middle East, are having an impact and we're seeing more attacks being outsourced to criminal networks. AI is also increasing the speed and volume of threats by lowering barriers to entry. We now have less sophisticated attackers capable of conducting more complex attacks.

But the same technologies can support our response as defenders. We're exploring AI adoption across the whole organisation, including in our security function, where technologies such as generative AI can boost our security posture.

AI security tools can help us do more than just detect, protect and respond. By removing some of the drudgery and repetitive elements of cybersecurity, like generating initial incident reports, they allow people to focus on the higher level, more expert aspects of their job. The frameworks we've got in place around responsible AI adoption are therefore informing how we plan and manage our workforce – and will develop in tandem with the technology over time.

Communication is critically important too. We're fortunate to have an executive team and board who understand and invest in cyber security. But, in every organisation, talking clearly to senior leadership about cybersecurity, and it's impact to the organisational strategy, is the best way to get their buy-in to get things done. We also talk continuously with the workforce. We run mandatory training course across the organisation covering things like phishing and malware, and we create targeted education and awareness campaigns based on the types of attack getting the highest click rates at any given moment in time.

It's still early days and change is constant. But I feel like we have solid foundations in place.

Alister Shepherd
Chief Information Security Officer
Financial Conduct Authority

Chapter 4

A blueprint for UK success

For the UK, boosting the number of organisations that are resilient to AI-enabled cyber threats is a priority.

Indeed, as we have seen in previous chapters of this report, the nation's long-term growth and competitiveness depend on it.

This requires strong, forward-thinking leadership at a national level. Building on the positive signs at the AI Safety Summit, the government must now seize the opportunity to position the UK as an international hub for AI innovation, progress and talent.

But how? What actions can political leaders and policymakers take to bolster the UK's collective cyber defences and, in doing so, create a launchpad for achieving its goal of global AI leadership?

Here is our blueprint for the nation's AI cybersecurity success:

1 Support widespread adoption

The UK is already leading the way on the responsible development of AI, calling on countries to commit to making the technology resilient by design. And rightly so. Every day, Microsoft detects more than 65 trillion cybersecurity signals but, thanks to AI, we now have the power to adapt alongside these evolving risks, detect anomalies instantly, respond swiftly to neutralise them and tailor defences for an organisation's individual needs. The widespread use of graphics processing units (GPUs) will help here, enhancing the performance and efficiency of AI solutions. But there must also be a more pronounced focus on fostering democratic inputs into AI development, while drawing on and replicating programmes like Innovate UK's £54 million research funding to develop secure AI that can help solve major safety challenges. The ultimate goal must be ensuring the highest possible levels of security through the widespread adoption of AI-enabled defences, while inspiring ever more creative cyber approaches among the nation's security professionals at the same time.

> "AI can inspire creative thoughts and ideas within an organisation that perhaps wouldn't have occurred otherwise, including uncovering new ways in which criminals might attack it. Cybersecurity professionals tasked with working out what malicious actors might do can then use this enhanced creative thinking to develop better methods for stopping them."

Duncan Anderson
AI expert and Founder
Barnacle Labs

2 Target investment

Investment in cyber resilience drives opportunity and growth—and vice versa. To the point that more than half (55%) of UK organisational leaders worry that a lack of spending on cybersecurity could hold back the country's economic progress. This investment (and the risks it aims to mitigate) must therefore be prioritised and precise, with organisations encouraged to focus on buy-and-build configurations or off-the-shelf solutions. Likewise, money must be spent on developing secure sandboxing environments where innovative ideas can be tested, refined and rolled out quickly.

"Every risk register I see has cyber as the number one risk yet that doesn't necessarily translate into an investment portfolio to address it. Other risks around market expansion, growing customer base and driving profits tend to be focused on first. It's not sustainable."

Karl Hoods
Chief Digital and Information Officer
Department for Energy Security & Net Zero and Department for Science Innovation & Technology

3 Cultivate talent

The UK regularly over indexes on benchmarks for cybersecurity resources. It also boasts one of the world's most talented cyber workforces and a market-leading position in research, entrepreneurship and AI innovation. Yet organisations still report challenges attracting and retaining skilled workers, meaning only 35% can fill permanent cybersecurity roles in-house. This lack of human resources stops them from capitalising on new opportunities—both individually and collectively. The key to addressing this challenge lies in using nationally incentivised skills programmes, on-the-job learning and public-private partnerships with academic institutions to better cultivate nascent human capital while ensuring talent is equipped to deal with future challenges as well as present ones. Here the recently launched grant scheme for small- and medium-sized businesses, the £100 million of government funding aimed at accelerating the use of AI in life sciences and the £118 million AI skills package represent a great start to build on and extend in future.

"When students come out of university, they have various skills but not necessarily the ones the industry needs. Universities have to do more than just train the workforce to be 100% ready to deploy AI solutions now. We must give people the understanding to develop and apply their knowledge to future problems. Academia and business need to work together (as well as with the government) to create thinkers rather than only doers."

Luca Viganó
Head of Cybersecurity Group, Department of Informatics
King's College London

4 Foster research and knowledge sharing

At the heart of progress is collaboration not competition. The UK must continue to invest in public/private R&D partnerships while supporting entrepreneurs to innovate on AI's frontier. Most importantly, breakthroughs should be open sourced across business, government and academia, with incentives for publishing discoveries so others can benefit from and build on them. Likewise, learnings from cyberattacks should form the basis of nationwide, cross-industry alliances for cybersecurity preparedness, turning threat awareness into readiness and, ultimately, mitigation. If needs be, this culture of knowledge and best practice sharing could be supported by explicit government regulation.

"Technologies like generative AI and machine learning are very new in terms of how we implement them. A lot of algorithms and a lot of technology have been kept inhouse. But the good thing is that there is a very good collaboration between fintech companies in terms of cybersecurity knowledge. We tend to share our approaches much more than many might think. And then we can take advantage and share the ideas. That's how we all progress together."

Dr Diego Sempreboni
Research Associate
Department of Informatics
King's College London

5 Lead on governance

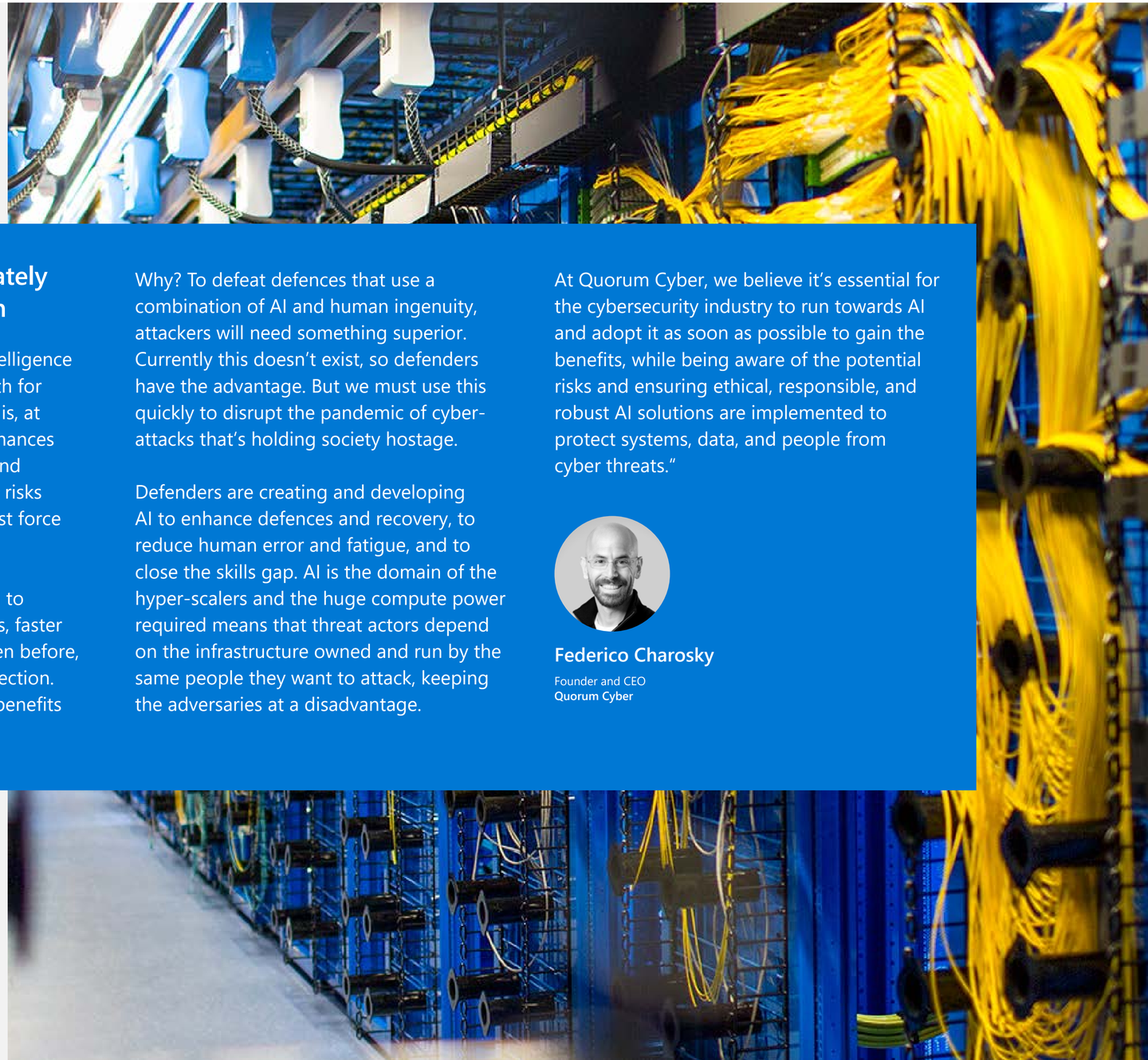
As we have discussed already, the UK has so far done an impressive job of positioning itself as a worldwide leader in both responsible AI and cybersecurity and helping to ensure there is a consistent standard for organisations in the UK and internationally, as evidenced by the *Guidelines for secure AI system development* recently published by The National Cybersecurity Centre. Policymakers should continue to collaborate with businesses of all sizes and across all sectors — from healthcare to manufacturing, and from the military to finance — helping them operationalise simple, outcomes-based guidance that encourages the safe deployment of AI in cybersecurity.

"There is momentum within the UK government to fix the multiple layers of readiness for relevant critical technologies development, cybersecurity development and use that to leverage international collaboration and international bilateralism. This will build the foundation to foster a global culture of trust, global and national capacity development and information sharing amidst public and private sectors not just in the UK but globally and build a multiplier effect through an active worldwide network of allies and partners."

Prof. Hoda Al-Khzaimi
Director
EMARATSEC Center for Emerging Tech and Advanced Research Acceleration in Security, AI and Cryptology

Of course, these steps are just the beginning. The UK's ability to stay at the forefront of AI's future will rely on how well it can evolve and adapt to the ever-extending capabilities of the technology itself—and the risks they carry.

Yet what will not change is the need for the ambitious vision of national leaders to be backed by progressive actions from the country's businesses. In the fifth and final section of this report, we therefore provide a second blueprint. One that lays out exactly how organisational leaders can improve their own cyber resilience and, in doing so, help the UK leapfrog the world on the path to AI leadership.



How AI is disproportionately helping good people win

"Like any technology, artificial intelligence (AI) can and will be leveraged both for good and bad. This is because AI is, at heart, a productivity tool, that enhances the capabilities of professionals and organisations, while creating new risks and attack vectors. It's the greatest force multiplier this industry has seen.

Threat actors are already using AI to launch more sophisticated attacks, faster than ever and at a scale never seen before, while enabling them to avoid detection. However, AI will provide greater benefits to defenders than attackers.

Why? To defeat defences that use a combination of AI and human ingenuity, attackers will need something superior. Currently this doesn't exist, so defenders have the advantage. But we must use this quickly to disrupt the pandemic of cyber-attacks that's holding society hostage.

Defenders are creating and developing AI to enhance defences and recovery, to reduce human error and fatigue, and to close the skills gap. AI is the domain of the hyper-scalers and the huge compute power required means that threat actors depend on the infrastructure owned and run by the same people they want to attack, keeping the adversaries at a disadvantage.

At Quorum Cyber, we believe it's essential for the cybersecurity industry to run towards AI and adopt it as soon as possible to gain the benefits, while being aware of the potential risks and ensuring ethical, responsible, and robust AI solutions are implemented to protect systems, data, and people from cyber threats."

Federico Charosky
Founder and CEO
Quorum Cyber

Chapter 5

A blueprint for organisational success

Let's start by reminding ourselves how UK organisations are faring when it comes to embedding sophisticated AI-enabled cybersecurity at the heart of their operating strategy. Or as Prof. Hoda Al-Khzaimi puts it: to becoming "resilient by design".

According to the research model, right now just 13% can be considered Resilient to cyberattacks. This small handful of organisations are characterised by making cybersecurity a true business priority, by a strong commitment to innovation and skills, and by trusted, transparent relationships with internal and external stakeholders.

Elsewhere, 48% are classed as Vulnerable, with limited cybersecurity best practices in place but without the necessary knowledge, skills and investment required to achieve full resilience. Meanwhile, for the 39% of organisations deemed At High Risk, the likelihood of falling victim to increasingly networked, motivated and well-resourced cybercriminals is most acute of all. Here, cybersecurity is rarely a business priority, threat monitoring and assessment are scarce and there is little investment in technological innovation and skills.

Shifting this balance towards widespread resilience is paramount—both to organisations' own individual success and to the prosperity of the nation's economy as a whole. And while the transition cannot and will not happen overnight, there are some immediate steps leaders can take to strengthen their cybersecurity and accelerate their journey to becoming resilient by design.

Clearly for At High Risk organisations, the need is most pressing. The financial, operational and reputational costs of successful attacks are a real and present danger. Indeed, around two in five (39%) senior decision-makers admit they are concerned about economic damage caused by a breach with the same number also concerned about the impact on their standing with stakeholders. Both figures rise to 48% among senior security professionals.

In **Figure 4,** we therefore lay out a series of immediate actions that leaders of these organisations can take to move forward and improve. Then in **Figure 5,** we do the same for Vulnerable organisations seeking to become Resilient.

Figure 4
Moving from At High Risk to Vulnerable

- Assess and understand the unique threat landscape for the business; AI investment helps with this and can provide simulation opportunities
- Create a plan for recovery and business continuity after an attack
- Understand the connection between business growth and cybersecurity resilience
- Use safe spaces for experimentation to overcome any fear of AI and create a culture of understanding and trust for employees at all levels
- Access tools using AI to detect and mitigate risk as a priority
- Budget for technological upgrades and cybersecurity costs, ensuring that the recovery plan is included
- Understand the talent requirements for an AI-enabled workforce, then look to the technology itself or to in-house training to build the required skills

Figure 5
Moving from Vulnerable to Resilient

- Make cybersecurity a core business priority
- Commit to adopting AI more broadly in the business
- Move from understanding AI to proactively innovating with it
- Focus investment on technological upgrades and new AI-enabled solutions
- Embed tools using AI to detect and mitigate risk
- Use AI to bridge the skills gap and talent shortage in cybersecurity
- Provide opportunities to elevate existing staff's skill sets and education around AI through on-the-job learning and personalised training
- Invest resources in a business continuity plan to speed up response time to attacks
- Deepen understanding of the skills required and hire/train in-house talent to focus on cybersecurity

"In recent years, easy access to artificial intelligence has enabled businesses to drive the next wave of digital innovation and it's exciting to watch. Adversaries with access to open-source models have been able to improve their current activities, such as phishing, and reduce their barriers to entry with coding assistance. Innovation and investment from organisations such as Microsoft are also allowing all organisations to address the skills gap by developing Copilots that assist their security teams, reducing the time and effort required to respond to threats and incidents.

In order for Britain to continue to be positioned as a global cybersecurity leader and develop itself as a superpower in AI, we must continue to drive the economy and our clients to develop grass roots talent and support them with tools such as Copilot for Security.

Within the security space, this will allow us to address the skills gap though blending both people and technology.

Undoubtedly, as the open-source capabilities of AI continue to improve, they will be used by all business models and organisations for both positive and negative actions. As such, we must have AI at the forefront of our minds and have strategic initiatives in place that will allow us to continue developing these capabilities at a pace and remain secure as a global community."

Martin Riley
Director of Managed Security Services
Bridewell

Wherever you and your organisation are on this journey, the most important thing is to be constantly moving forward.

As little as two years ago, AI remained a largely quiet influence in the world's daily life, often working unseen in the background of our homes, offices and devices.

Yet now all that has changed. As the technology becomes an ever more visible and integral part of government, business and society, it presents both novel risks and extraordinary opportunities. For organisations across sectors, success, survival even, relies on addressing both.

First and foremost, embracing AI-enabled cybersecurity offers UK organisations a way to mitigate the threat of attack and tip the scales back in their favour against criminals. This is proven to have a powerful impact on everything from their stakeholder relationships and workforce productivity to their market reputation and bottom line.

But more than that, it offers a solid platform from which to drive forward, setting the stage for organisations to unlock new cybersecurity markets, attract top talent, accelerate innovation and take a genuine leadership position on the global stage.

As Antonio Guterres, United Nations Secretary General, said in the aftermath of the AI Safety Summit: "The speed and reach of today's AI technology are unprecedented but the paradox is that in the future it will never move as slowly." If the UK can get ahead of the game today, a superpowered tomorrow awaits.

Chapter 6

Appendix

Methodology

The research included in this report was conducted by Microsoft in partnership with Dr Chris Brauer, Director of Innovation, Goldsmiths, University of London between December 2023 and March 2024 and included a core team of economists, psychologists, data scientists and social scientists from Symmetry. They used a mixed method approach to build a model, scorecard and blueprint of AI-enabled cybersecurity in the UK.

Literature review and model development

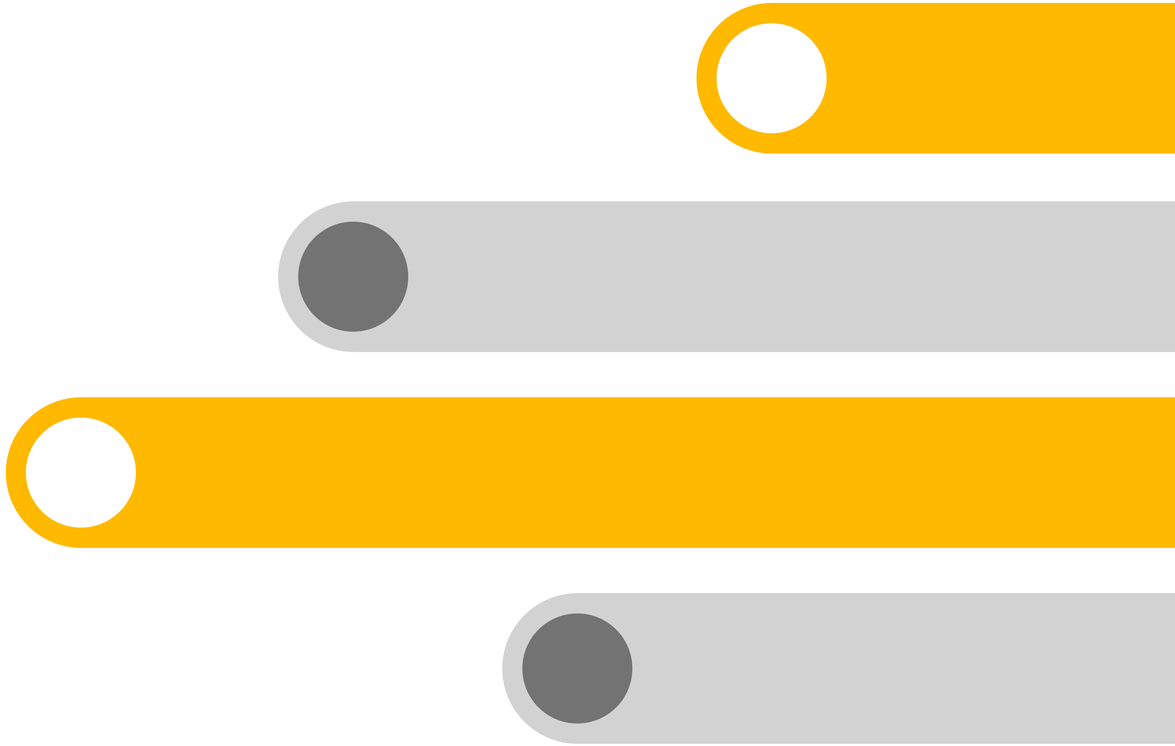
The process began with an in-depth review of academic, industry and media knowledge and data sources, which helped uncover the state of cybersecurity in the UK and, in particular, its relationship to the rapid progression of AI. From this, the research team developed a model through which to consider and score organisations' cybersecurity. This model includes six key dimensions: three behaviours and three capabilities.

Survey

Insights from this initial phase were verified quantitatively through barometer surveys conducted online by YouGov during December 2023 and January 2024. These surveys spoke to 1,039 senior business decision-makers, including 200 senior security decision-makers, as well as 1,051 employees from UK organisations of varying sizes, revenue distributions and industries. Unless otherwise stated, the data from each survey were kept distinct in the descriptive statistics included in this report. However, they were combined for the calculation of costs and the creation of the scorecard.

Qualitative exploration

The research team interviewed a variety of subject matter experts, including industry experts, cybersecurity consultants and academics. Their insights were used to inform both the research model and findings of this project. Quotes were analysed and used as evidence to support hypotheses and construct the blueprints for success.



Subject matter experts

Prof. Hoda Al Khzaimi
Assistant professor in Department of Engineering NYUAD
Director, Centre for Cybersecurity;
Founder and Director, EMARATSEC center for emerging tech and advanced research acceleration,
Associate Vice Provost of research translation and innovation New York University
Abu Dhabi United Arab Emirates
Cochair of global future council for Cyber Security on the World Economic forum

Dr Diego Sempreboni
Research Associate, Department of Informatics,
King's College London

Duncan Anderson
AI expert and Founder,
Barnacle Labs

Karl Hood
Chief Digital and Information Officer,
Department for Energy Security & Net Zero and Department for Science Innovation & Technology

Luca Viganó
Head of Cybersecurity Group,
Department of Informatics,
King's College London

Paul Kelly
Director, Security Business Group,
Microsoft UK

Jonathon Ellison
Director for National Resilience and Future Technology,
The National Cybersecurity Centre

Customers and partners

Federico Charosky
Founder and CEO,
Quorum Cyber

Jonathon Ellison
Director for National Resilience and Future Technology,
The National Cybersecurity Centre

Ffion Flockhart
Global Head of Cybersecurity,
Allen & Overy

Siân John
Chief Technology Officer,
NCC Group

Steve Mckeaveney
Head of Customer Success,
ITC Secure

Martin Riley
Director of Managed Security Services,
Bridewell

Alister Shepherd
Chief Information Security officer,
Financial Conduct Authority

David Wakeling
Partner, Head of Markets Innovation Group (IMG),
Allen & Overy

References

Stevens, T. [2018]. Global cybersecurity: New directions in theory and methods. Politics and Governance, 6[2], 1-4. https://doi.org/10.17645/pag.v6i2.1569

OECD [2015], Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document, OECD Publishing, Paris. DOI: http://dx.doi.org/10.1787/9789264245471-en

National Cyber Power Index: https://www.belfercenter.org/sites/default/files/2020-09/NCPI_2020.pdf

Global Cybersecurity Index: https://www.statista.com/statistics/733657/global-cybersecurity-index-gci-countries/

Global Cybersecurity Exposure Index: https://passwordmanagers.co/cybersecurity-exposure-index/#global

National Cybersecurity Index: https://ncsi.ega.ee/ncsi-index/

https://www.cybersecuritydive.com/news/ransomware-attacks-payouts-2021/622784/#:~:text=The%20average%20cost%20of%20a,the%20first%20half%20of%202021

Dubuis-Welch, C. (2023), 15 cybercrime statistics you ought to know: https://www.independent.co.uk/advisor/vpn/cybercrime-statistics

Navigating cyberthreats and strengthening defenses in the era of AI, February 2024: Cyber Signals (microsoft.com) https://news.microsoft.com/wp-content/uploads/prod/sites/626/2024/02/CyberSignals-Feb-2024.pdf

Gartner: https://www.gartner.com/en/newsroom/press-releases/2021-05-17-gartner-forecasts-worldwide-security-and-risk-managem

SonicWall: https://www.sonicwall.com/news/sonicwall-the-year-of-ransomware-continues-with-unprecedented-late-summer-surge/

UK Cybersecurity Breaches Survey: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2023/cyber-security-breaches-survey-2023

Insurance Times: https://www.insurancetimes.co.uk/news/uk-ransomware-attacks-rise-by-100-in-2021-rpc/1440698.article#:~:text=UK%20ransomware%20attacks%20reported%20to,by%20international%20law%20firm%20RPC.

Proofpoint: https://www.proofpoint.com/uk/resources/threat-reports/state-of-phish

https://www.gov.uk/government/news/levelling-up-push-sees-more-than-5000-public-buildings-plugged-into-high-speed-broadband

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1055565/Cyber_Sectoral_Analysis_2022_Report_V2.1.pdf

https://www.gov.uk/government/publications/uks-digital-strategy/uk-digital-strategy#s1-4

Young victims of cyberbullying twice as likely to attempt suicide and self-harm, study finds [2018] https://www.sciencedaily.com/releases/2018/04/180419130923.htm

https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/cyber-crime

An overview of catastrophic risks https://arxiv.org/pdf/2306.12001.pdf

Microsoft Security

To download the report please visit:

aka.ms/UKCyberOpportunity

Start again