ODGERS
WHERE LEADERSHIP MATTERS

Board Briefing:

Addressing the Challenges of Cyber Security in an Ever-Shifting Geo-Political Context.

Matt Cockbill Partner, CIO & Technology Officers Practice was delighted to talk with Jo Miller, National Security Officer for Microsoft UK, about the key issues of Cyber and Information Security facing Boards, and share her insights through this Board briefing.

Now more than ever, these issues are converging with strategic and Board-level risks around emerging technologies, societal changes and the skills demands on our global workforce, coupled with the increasing complexity and dynamism of the geopolitical landscape.

BACKGROUND

Jo is a national security professional, with a 25-year career in Security, Technology, and Defence. She brings perspectives rooted in geopolitics and reflects on the threats, and opportunities, that exist at its intersection with technology and security.

Earlier this year, Jo was delighted to join Microsoft as its National Security Officer in the UK, confident that Microsoft's established position as a global engineering innovator has the credibility, the focus, and the commitment to systems of security both within the organisation, and for external markets and partners across the global economy.

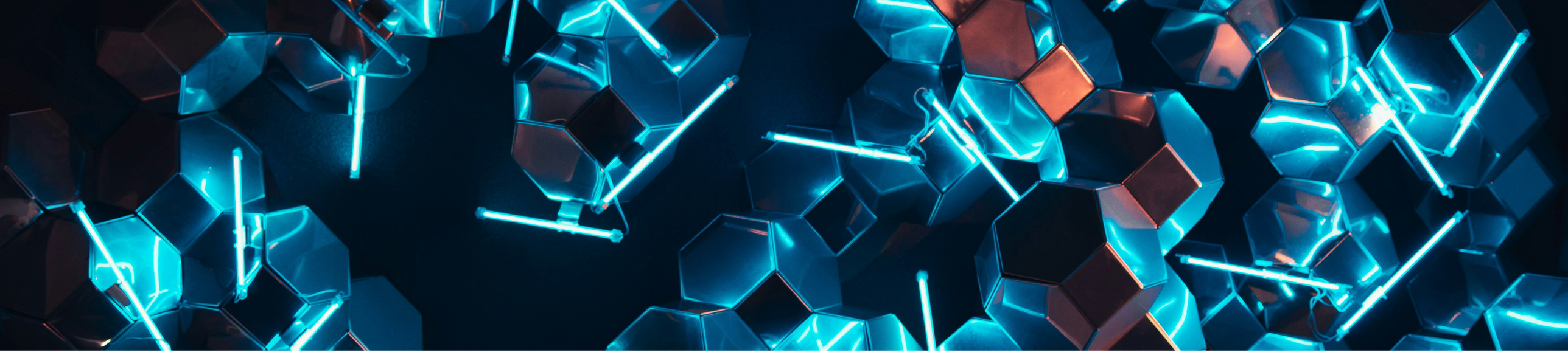
She emphasised throughout our discussion that now is the moment for the UK, its citizens, its businesses, and critically its senior leaders to not just wake up, but to step up and take action - recognising the convergence of geopolitical challenges with rapid technological advancements, and the market differentiator that security poses for Boards. The following notes are taken from their discussion.

LET'S START WITH A QUICK VIEW OF THE HERE AND NOW:

We are at a seminal moment where the geopolitical, technology and security landscapes are becoming more and more intertwined; and how we talk about that is key. Presently, the security industry uses a fair amount of fear-based language when we talk about security - be it cyber security, AI security or national security. We talk about threats, attack vectors, vulnerabilities.

This compels us to behave as we have done for millennia - to fight, to flee, or to freeze - and so we need to shift the narrative from one of fear, to one of safety, pragmatism, and action. From a distress-based, and stressful, position to one based in reason and well-managed risk; tending to those assets that we care the most about keeping safe and taking appropriate actions to do so.

> **In her new role, Jo is fortunate to be able to bring to bear her knowledge, expertise, and networks, having spent over two decades in the national security and defence ecosystem, in the UK and worldwide.**



She works with teams across Microsoft and closely with the UK public sector, and international partners to explore what security means for the UK. Setting out how Microsoft is delivering through its insights, its guidance based in world-class research, and a security-first mindset, to help customers and partners meet today's challenges head on in a way that is sustainable and resilient to the increasing dynamism of the geopolitical landscape. This is the environment that Microsoft builds for.

She described that security, in this context, takes different forms.

Cyber Security - where Microsoft builds and operates one of the most advanced security systems in the world. The scale of its investment in security is anchored in key commitments that Microsoft lives by, based in its 'Secure Future Initiative' (SFI).

Whether that be in its platforms, its people and their development, designing in security and setting it as a default in its products, or in its global reach, processing 78 trillion security signals each day to inform insights - security is front-and-centre and it has to be.

AI Security - the secure design, development and use of AI models and agents, of agentic AI and systems, and how those are integrated into your organisation's broader infrastructure, also features highly. It is shifting the scale and pace at which we, businesses and Boards, must tend to our security practices.

You need to know what assets you have and where they are, whether and how your on-premise servers interface with the internet, how open source AI models are being used inside your organisations, whether your policies discourage or prohibit this, to manage the emergence and risks of 'shadow' AI. And, as an example, this is where Microsoft's recent announcement to invest £22 billion ($30 billion) in the UK, to enhance AI infrastructure and operations, is critical - supporting business leaders in ensuring that their Cloud-based and AI-enabled operations are secure and safe.

FROM A CYBER SECURITY-PERSPECTIVE, THIS IS SIGNIFICANT AS THERE ARE WELL-KNOWN TECHNIQUES AND TRADECRAFT THAT EXPLOIT - BROADLY SPEAKING - COMMONLY UNDERSTOOD WEAKNESSES IN A NETWORK OR DEVICE.

> **AI raises the bar because it means this can happen at greater volume and at greater scale, across your organisation; automating reconnaissance on your networks, scanning for the weak points in our cyber and protective security.**

This for Jo is the key shift in the security landscape - it constitutes a challenging point of parity with the pace of change. And this is why we see national authorities across the UK and worldwide placing greater emphasis on the widening gap between our levels of organisational, and national, resilience, and the increasing scale and complexity of the security landscape.

This both excites and energises her as a security professional, and it constitutes a real call to action.

THE EVOLVING THREAT:

We can think of cyber actors as being on a spectrum, ranging from the less sophisticated or untargeted criminality, to online fraud or cybercrime, through to the targeted and more advanced actors and state-led tradecraft. For example, we see in the media the steady stream of headlines about a variety of companies ranging from retailers and consumer goods, insurers and financial institutions, academic organisations and local authorities, some of who's security postures have been breached by untargeted cyber actors. In this context a cyber actor seeks out weak points in networks or devices.

Elsewhere on that spectrum companies or organisations, or individuals, might be specifically identified and targeted by cyber actors with the intent to compromise them or their organisation; targeted ransomware attacks or exploiting software vulnerabilities and putting down web shells, a sort of foothold in the network, denying access to systems or accounts, or exfiltrating data for the purposes of IP theft or espionage.

And then at the far end of that spectrum, we see more complex security challenges, where a hostile actor or nation state might typically operate, drawing on significant and sustained investment in tradecraft and cyber capabilities.

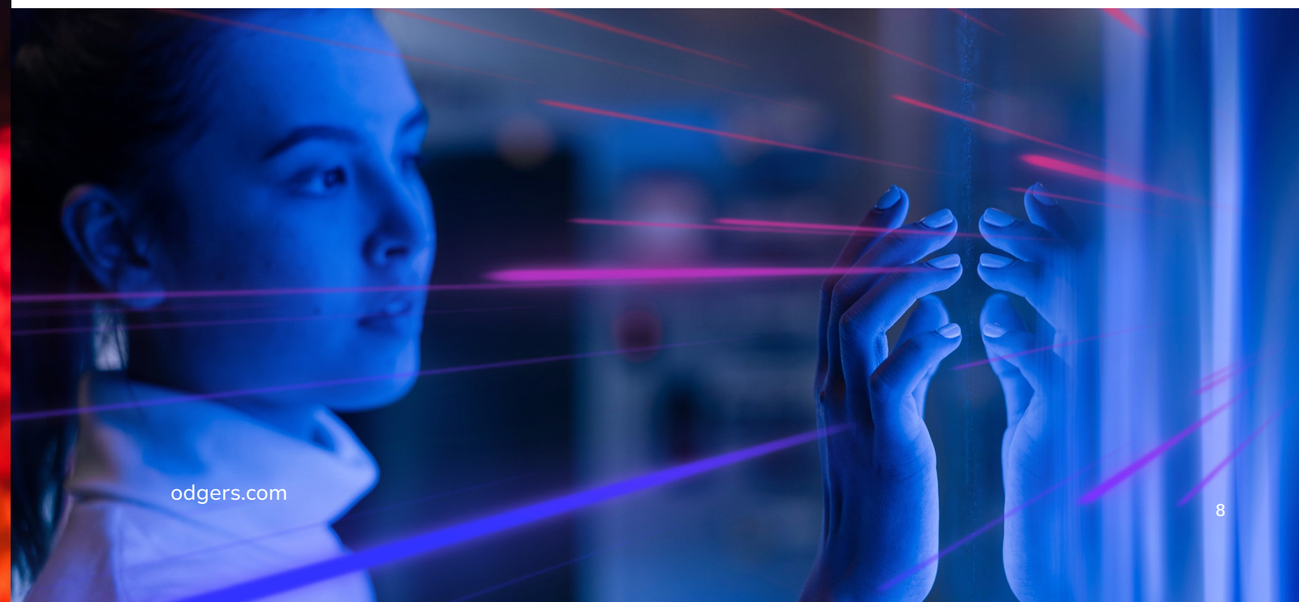
Such cyber actors might operate covertly for the purposes of intelligence or espionage operations, or might operate noisily or clumsily, either deliberately obfuscating their sophistication as a cyber actor or to make a point.

Typically, it is this spectrum that has helped national authorities and organisations identify and classify a given cyber incident or actor. What is interesting however is that the democratisation of these capabilities and this tradecraft - cyber proliferation, and AI is a key enabler of this - is bringing that spectrum around full circle.

What might appear to be an untargeted or criminal act in cyberspace might in fact be a more sophisticated actor operating via a proxy. And so the barrier to entry lowers - cyber capabilities are becoming more readily-available and accessible, AI-enabled tradecraft means such actors have greater reach and can operate at scale, and the sophistication of the attack is not an indication of the intent, or identity, of the true actor.

THIS CYBER SPECTRUM BECOMING A FULL CIRCLE MEANS THAT BASIC CYBER HYGIENE AND WAKE-UP CALLS ARE SIMPLY NOT ENOUGH, WHETHER FOR THE UK PUBLIC SECTOR, THE UK CNI (CRITICAL NATIONAL INFRASTRUCTURE) OR THE CNI-ADJACENT.

Arguably that constitutes the near-entirety of the UK. ‘Cyber Essentials’ was essential when it launched in 2014 and over a decade later, given the changes and shifts Jo sees, having a robust underlying foundation of cyber hygiene is now the absolute bare minimum. And what she is most curious about is the aggregate risk to the UK, to the UK’s resilience; these cyber attacks are in part about theft and ransom payments and espionage, and they are in part about the aggregate impact on the UK and confidence in our collective resilience.



Again, given the complexities of the geopolitical landscape and the importance of the UK's soft power, and its global reputation as a research and innovation powerhouse, especially, we all share in the responsibility to keep the country and its people safe. That's us; that's on all of us.

In the UK, Jo shared that we have globally-recognised national authorities for cyber security (the UK's National Cyber Security Centre), for protective security (the National Protective Security Agency), for AI security (the AI Security Institute), and a world-leading diplomatic service for whom both the UK's growth and its security is front-and-centre of our global relationships.

Engineering companies, like Microsoft, and other suppliers and partners, offer free and evidence-based guidance and materials that are designed to help Boards and senior leaders better understand and act on these issues.

Not out of fear or distress; out of good reason, safety, and shared responsibility, and from an informed position.

Each year, Microsoft publishes its 'Digital Defence Report', setting out these challenges and opportunities, it shares its annual 'Responsible AI Transparency Report', its Cyber Security Assessment Tool, and a range of AI assessment tools are also readily-available on Microsoft's website.

The Shifting Geo-political Context:

But of course this threat landscape, evolving as it is, doesn't exist in isolation - it exists in a broader geopolitical and economic context. We are, right now, in a period that is as fascinating as it is alarming. Our political landscape is shifting; we are seeing electorates across Europe, the Americas, Asia and further afield shift from centrist politics to right of centre, which is manifesting in electoral outcomes and in polling results.

With changing administrations and political norms, comes a shift in prevailing foreign policies, and as such, the profile and importance of trusted and established institutions, academic bodies, and the role of multilateral alliances such as the UN and NATO, is evolving. Some diminishing and some increasing in importance.

WE SEE THIS IN GLOBAL RESOLUTIONS LAUNCHED TO PROMOTE INTERNATIONAL COOPERATION ON AI GOVERNANCE AND INDEPENDENT SCIENTIFIC ANALYSIS OF AI RISK, AS THE UN ANNOUNCED RECENTLY.

We also see this in the demands being made of alliance members, to explicitly increase their % of GDP spend on defence, which in turn impacts on national spending, on social expectations, and on costs of living.

With this comes greater opportunism - nation states and leaders pursuing their own national goals, at the expense of, or sometimes irrespective of, the direct or indirect consequences felt elsewhere, and with or without the support of partners.

Many current examples come to mind: Russia's willingness and confidence to pursue its territorial goals across Northern Europe; Israel and Iran, and the broader Middle East, and developments in East Asia and the South China Sea, with China having made explicit its ambitions and aspirations. Clearly, we are seeing a continuing security bifurcation across the East and the West.

Technologically speaking, some of the technologies developed outside of the West are done so indigenously and so the threats to our information and digital infrastructure risk becoming increasingly opaque, which poses challenges both to the historic Western dominance of global security and technology markets.

As it becomes increasingly difficult to get ahead of security challenges in this context, and as the threat landscape shifts and evolves, it becomes exponentially more difficult for organisations to secure themselves in cyber space and to build national resilience.

We are talking more about this widening gap, a key point that the UK's National Cyber Security Centre (NCSC) has repeatedly emphasised to businesses and the public sector; the gap between the threat level and a given organisation's resilience (or our national resilience) to that threat, having widened and continuing to widen. Unless we act. And we must act.

TAKING ACTION:

We hear repeatedly about breaches and cyber incidents, often described as "wake-up calls" where media coverage and leaders urge us all to take notice and lean into our responsibilities for cyber security. Fundamentally though we have reached the point where "wake-up" calls are not enough - taking notice and leaning in is not enough. We have gone far beyond that point.

THEREFORE, OUR LANGUAGE AND BEHAVIOURS NEED TO SHIFT FROM "WAKING UP" TO GETTING UP AND TAKING ACTION.

BOARD LEADERSHIP AND CYBER ACCOUNTABILITIES:

As members of Boards, we all carry fiduciary responsibilities - we know that. As Directors registered with Companies House, and equivalent authorities in other regions, we are legally, financially, and morally accountable for the health of the organisations that we have the privilege to govern, and the quality of the services and products that we deliver to our customers.

Again, we know that. This includes cyber security, however, the management of our enterprise security and the Board conversations and governance that we apply to our enterprise security.

And so, at a practical and pragmatic level, stripping back the fear-based language and the abstraction we hear around "wake-up calls", this is as much about liability and accountability, as members of Boards, as it is about morality and integrity.

That is a simple message and one that we as Board leaders should be embracing:

> **Understanding our liability and cyber risk, governing well and acting on it, and learning from those companies who didn't get ahead of their cyber risk and unfortunately are suffering the consequences publicly, in the media and in the court of social opinion.**

Actions That Boards Can Take:

1. OPTIMISE

Make complete use of the security licenses and terms of service that you already have in place (and are already paying for). Ensure that you have the appropriate security functions configured correctly, work with your service provider to do this.

2. CONSOLIDATE

Understand what security functions you have in place, such as a managed SOC, and which are duplicated. Perhaps you have multiple, duplicative, SOCs if you are a large organisation operating across different regions. Too often, businesses have multiple multi-vendor licences in place for the same function, and so consolidating these is an immediate (and cost-effective) route to better understanding, and therefore securing, your enterprise.

3. TARGET YOUR RESILIENCE MEASURES

Given this context, focus on (i) knowing what assets you have and managing the security of them, (ii) identity and access management, especially in the world of AI, and (iii) proactively get your enterprise and assets quantum-ready. Ensure that any new products or services you are procuring will be quantum-safe.

4. BUILD NATIONAL RESILIENCE

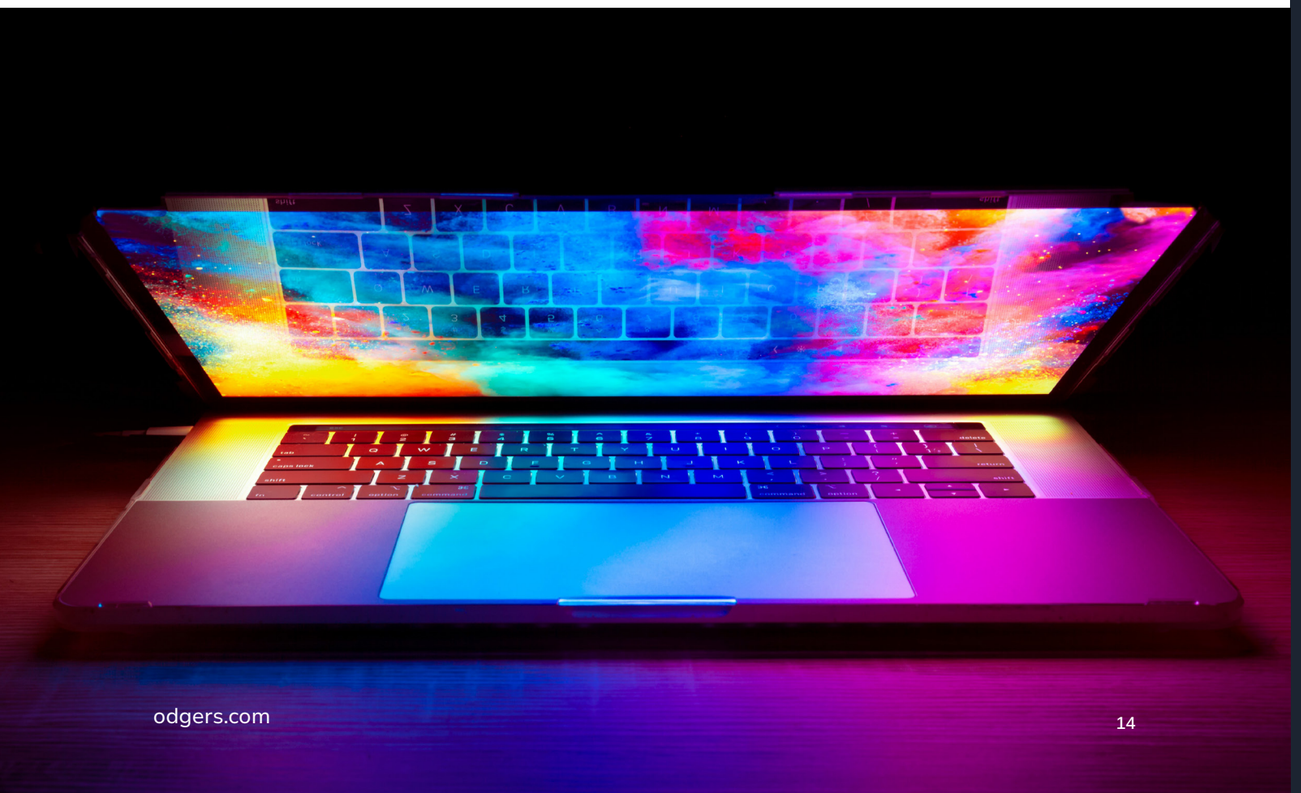
Again in this context, taking action to secure your enterprise is not just for the public sector or for those in the UK's CNI. Given the complexities of supply chains and our collective dependence on critical services and functions, we are all to a degree, what Jo calls, CNI-adjacent and so we all must take seriously our responsibility for building national resilience.

The NCSC reported in their Annual Review 2024 that over the last three years, they have seen a 20% increase in cyber incidents and a 44% increase in those that affect public services in the UK. And so enterprise security, or insecurity, irrespective of whether your organisation is part of the CNI, will have an indirect impact on our national resilience. This necessitates clear and oft-rehearsed crisis management, well-understood incident response mechanisms, whether in-house or better-optimised as per the first point.

Rightly, engineering innovators like Microsoft build for this environment - it has one of the most advanced, world-leading, security systems in the world, with AI integrated to better automate security operations, and so Jo has confidence and hope for a secure future. One where we all play our part in safeguarding our enterprises and assets, and in building our national resilience.

To do so, we must all optimise and consolidate, target our enterprise measures, and take responsibility for our shared mission in building a resilient and secure UK, set against this shifting context and threat landscape.

NOW IS A REAL MOMENT IN NATIONAL AND GLOBAL SECURITY, WE ARE ALL ACCOUNTABLE, AND WE WILL ALL BEAR THE COSTS OF INACTION; THIS IS A MOMENT THAT IT WILL GENUINELY TAKE US ALL, COLLECTIVELY, TO MEET.



Guest Author:

Jo Miller

National Security Officer
Microsoft UK

Jo Miller is the National Security Officer at Microsoft UK, and a career security and technology professional. She has held various senior executive roles across the public sector, primarily in national security and defence, as Director for Serious and Organised Crime, and then Chief Data Officer in the Home Office, specialising in the intersection between security, technology, and geopolitics.

She holds a range of non-executive Board roles, is a Trustee at UCAS, a NED on the Board of the UK's national governing body for snowsports, and Chair of the Board of the UK's flagship regional cyber ecosystem, a community-interest company comprised of over 5,000 members.

Our Author:

Matt Cockbill

Partner, CIO & Technology Officers
Odgers

Matt is a Partner in the Odgers CIO & Technology Officers Practice. He specialises in recruiting CIO, CTO, CDO and CISO appointments cross Aerospace & Defence, Engineering & Manufacturing Energy & Utilities markets, working with FTSE listed businesses through to series A businesses. He has more than 20 years' experience in recruiting digital, data and technology enabled transformation leaders both in the UK and Europe.

ODGERS

Where Leadership Matters.

odgers.com