CHIEF DISRUPTOR

TANIUM

The Interconnection between People, Process and Technology

Welcome to "The Interconnection between People, Process and Technology: A Reality Check on IT Complexity, Security Resilience and the Dawn of Automation and AI".

In an ever-changing world of lightning-speed technological advancements and unprecedented connectivity, the role of IT and security leaders has never been more important. With complexity seeming to multiply year on year, this office has become integral to not only security and operational resilience but also to business growth in the digital age.

Organisations are rapidly adopting AI and automation tools to enhance threat and anomaly detection, and to automate response systems. This is driven by the increasing frequency and sophistication of cyberattacks which are fuelled by emerging technologies like AI, IoT and Quantum Computing.

However the journey to ROI from these new technologies is proving to be far more challenging than first anticipated for many business leaders. Many are discovering that despite significant investment and effort, initiatives and new tooling may fail to scale beyond prototype to production and ultimately become a significant cost versus bringing return.

In this research piece, we wanted to understand the reality of being an IT leader in fast-moving and often unforgiving modern world. In order to give you that depth, we conducted 23 in-depth, qualitative interviews with industry leaders from a broad range of organisations from around the globe.

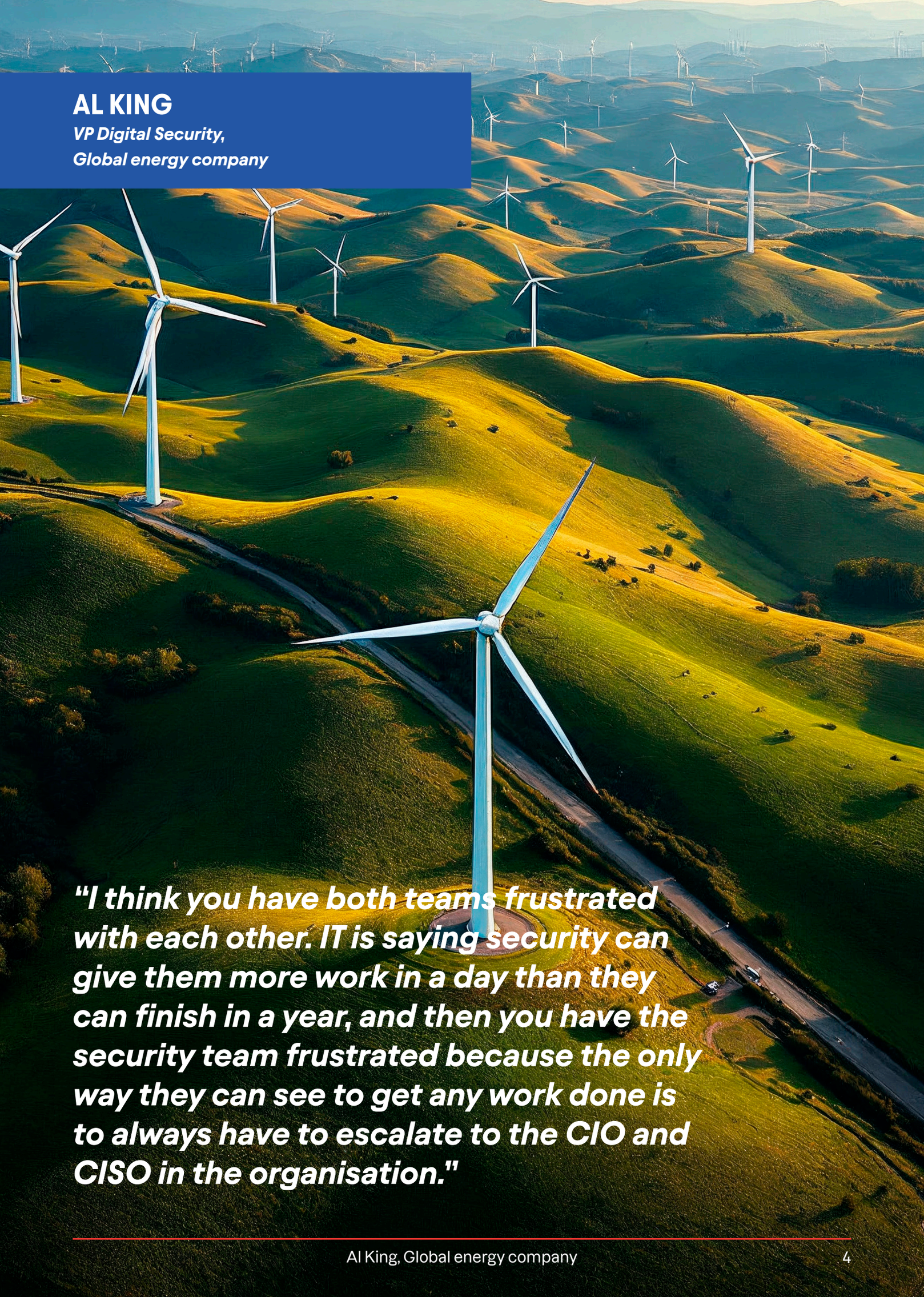
Despite the broad range of industry sectors and experiences outlined in the interviews, key trends were observed that will make interesting reading. Importantly, there was agreement that without building strong foundations in each of these areas, organisations would struggle to scale prototypes, integrate new technologies and ultimately achieve business success.

We have thoroughly enjoyed talking to this accomplished group of IT and security leaders and innovators, and would like to thank them for contributing to this important research. In addition, I'd like to thank the Chief Disruptor team, and in particular Caroline Boyd and Alexa Pherez, for their significant contributions in helping bring this book to fruition.

I hope you'll find these real-world experiences useful and informative.

Emma Taylor
Founder & Managing Director, Chief Disruptor

Contributors



AL KING
VP Digital Security,
Global energy company

"I think you have both teams frustrated with each other. IT is saying security can give them more work in a day than they can finish in a year, and then you have the security team frustrated because the only way they can see to get any work done is to always have to escalate to the CIO and CISO in the organisation."

Heading up Digital Security in an organisation transitioning from an integrated industrial oil company to an integrated energy company can be very rewarding.

"It's just kind of nice to be driving along and seeing an EV charging station and knowing it's secure, and knowing that you and your team have put the work in to help it be secure."

But it's also highly challenging, Al explains, because leaders are often forced to juggle multiple competing priorities; balancing both the business need and the sheer number of vulnerabilities that organisations face today. It's this perfect storm that he believes can encourage silos within IT security and IT operations.

"I think you have both teams frustrated with each other. IT is saying security can give them more work in a day than they can finish in a year, and then you have the security team frustrated because the only way they can see to get any work done is to always have to escalate to the CIO and CISO in the organisation."

Like many IT and cybersecurity leaders, he can already see tangible benefits from AI and automation taking over some of the mundane tasks that left analysts feeling burnt out and overwhelmed.

"It's really reducing the fatigue that we're seeing on our security operations center (SOC) analysts and it helps them focus on the key important things. It's reducing a lot of the fatigue and burnout that we're seeing in those groups where they are having to go and chase down the numerous vulnerabilities and attack services that are out there. And, what we're seeing is the tooling really being able to take alerts, take the signals, put information together from different sources and then give them something that they can work with."

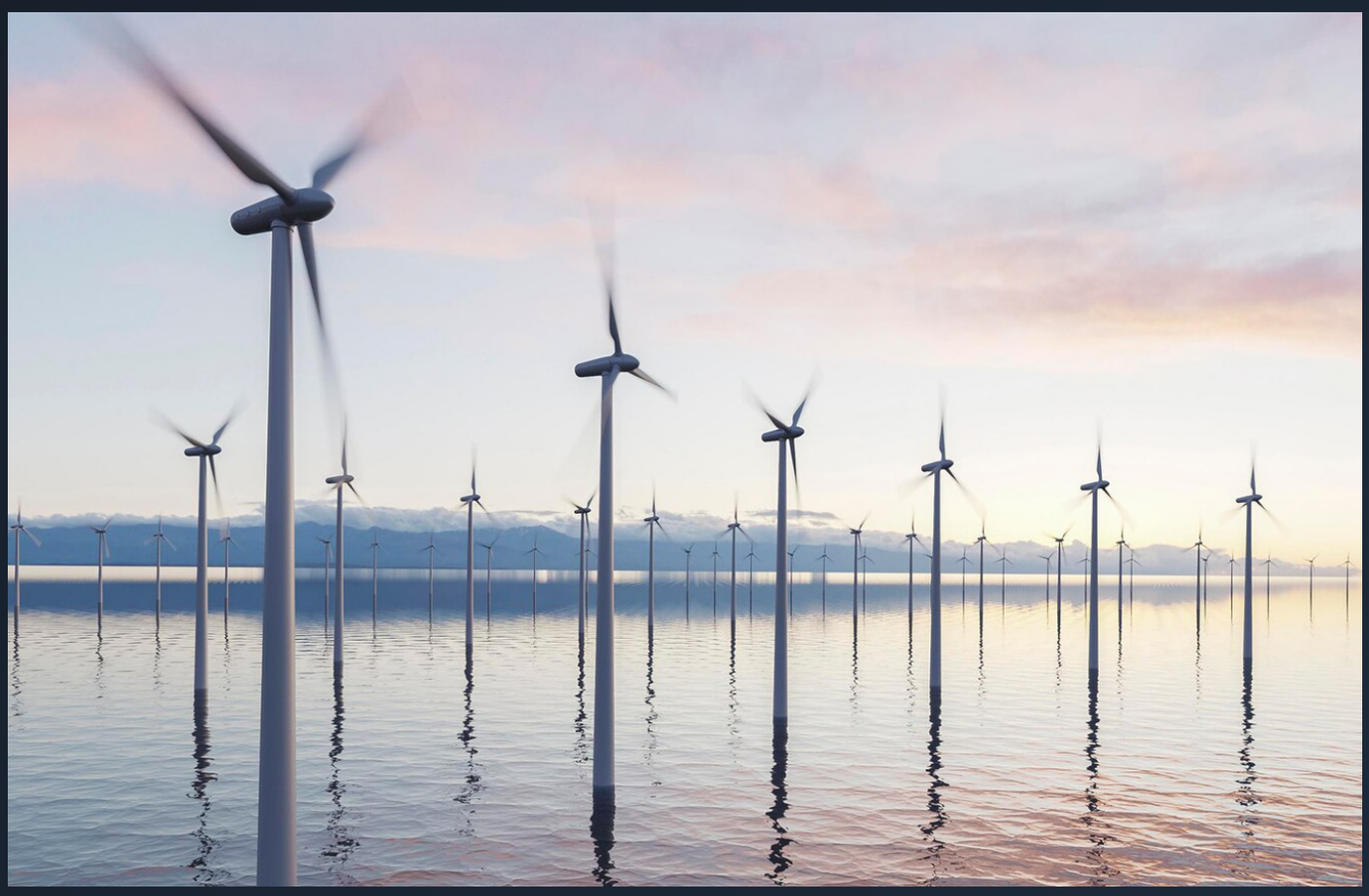
But technology is, he argues, just part of the solution and he suggests that both IT and cybersecurity teams should also re-evaluate their ways of working.

"Firstly IT and cybersecurity teams have got to agree on how to prioritise vulnerabilities. If everything is important, nothing is important, including IT operations to help drive and agree on accountability and timelines, and don't just focus on vulnerabilities. Just focus on the ones that are out of compliance, that will relieve the stress on the IT teams and make

the security teams feel like they are making traction within the business. Then you have also got to bring the business along on that journey because you've got to build hygiene into the way they work. Both teams have got to celebrate the small wins to drive the correct behaviours and create those ongoing behaviour changes that you're looking to build within the organisation."

When it comes to the important issue of the IT and cybersecurity skills gap, he acknowledges that the gap is there but also points to a disconnect around definitions and acronyms used in the security field, and calls for clearer terminology and communication to avoid confusion.

"The onus is on the security teams to build those functional requirements so that those teams can understand them... but we don't have the right nomenclature out there so we use terms interchangeably. Nobody knows what they mean. We all run around trying to figure out digital transformation, what is that? Is that just the lift and shift from on-prem and going to the cloud? Or what do we mean by that when we say we want to go through a digital transformation?"



ANDY PIPER

CISO Investment Bank & Markets, Barclays

"The risk of AI-powered attacks are inevitable, and when they come at machine speed, our defence must be AI-powered too."

Andy is the CISO for the Investment Bank & Markets division at Barclays, covering everything from investment banking and wholesale lending to research. He began his career in professional services at Deloitte, specialising in technology risk across a wide range of clients, before focusing more on financial services and finally moving to one of his clients, Barclays.

Andy's greatest aspiration is to redefine the perception of security, and to move away from the old idea of the CISO as "the House of No" towards that of empowering the business to succeed, securely and responsibly.

"I want my team and me to be seen as enablers, not blockers. That means working in partnership with the business, aligning our goals and strategies. The default answer to the business should be "yes, with the right controls in place."

Andy believes there is a widespread skills and talent gap across the industry, with a growing number of unfilled cybersecurity roles. But rather than technical, Andy argues that the skill most important to the CISO is communication.

"It's essential for a CISO to be able to explain complex cybersecurity topics to non-technical stakeholders, like boards or regulators in terms they understand. Boards care about how cybersecurity affects strategic goals, risk and business operations, not the technical minutiae. While we rely on SMEs for deep technical input, a CISO must be the translator and strategist."

Given the nature of the financial services industry, regulatory compliance is a big concern. Indeed, operating in over 40 countries, the team is required to manage more than 74 regulators.

"Each country we operate in has unique cybersecurity requirements, some overlapping and others conflicting. Managing and staying compliant with all of them is a full-time job. Even incident reporting varies with some regulators expecting notification in minutes, others in hours and some when there's a meaningful update. That deeply affects our incident response processes globally."

Structured processes are key to not only managing cybersecurity internally, but also to handling the regulators. This includes horizon scanning for upcoming regulatory changes, engaging with consultations and white papers, and adapting technology proactively. Firms are also required to periodically meet with regulators, quarterly, bi-annually or annually which requires a dedicated team to prepare responses.

"Communicating effectively with regulators is a key skill in itself. Again, it's about translating technical realities into accessible, accurate narratives."

Andy makes the point that AI itself is not new to the financial services industry which has used algorithmic trading for over a decade. He feels that the industry is comfortable with AI when it's secure, transparent and well-regulated. However, he also believes that AI is reshaping the cybersecurity landscape in three key ways. The first way being the speed of adoption.

"Generative AI has exploded in usage, and that pace is creating a gap and we're all playing catch-up. It's in everything now, and we often have to disable vendor tools that use AI because we can't verify their security posture, which ties directly into compliance."

Another observation is what he describes as the dual-sided security challenge; both the challenge of securing new AI tools and using AI for security.

"We're asking tough questions: where does user input go, is it stored, is it used to train models and can we trust its output? We don't want sensitive data like PII or IP going into tools we can't fully control or audit. Conversely, AI could be used to help to sift through billions of daily security events to identify real threats, highlighting the operational value of automation."

Andy also warns of "New Threat Vectors" being used by attackers to bypass existing security measures and gain unauthorised access to systems or data.

"AI-generated phishing is nearly perfect; the grammar, tone and the structure. This is rendering traditional email threat training obsolete. Model poisoning is another real threat with malicious actors influencing how AI systems behave."

HOSANNA OUELLETTE

Director of Global Program Management, Spotify

"Oftentimes, processes get a bad rep because they are an afterthought or bogged down by organisational debt. Invest time up-front to be clear on outcomes and instrument your process with success metrics so you'll know if you've got it right."

Since its launch in 2008, Spotify has grown rapidly in terms of users, revenue and advertising, and currently has over 600 million users and 263 million paying subscribers worldwide. Perhaps inevitably, when start-ups scale rapidly, the internal systems that have evolved organically, become inefficient or redundant. Indeed, Hosanna explains that at one stage, Spotify had 17 different tools in use that were creating business silos and complexity.

Hosanna believes in taking a design-driven approach to solving user challenges, and with this mindset, implemented a centralised work management platform to consolidate these 17 different tools into one. The initial implementation brought immediate wins, like a shared language across teams and a single source of truth accessible by leadership and global teams. But Hosanna concedes that it's an ongoing journey with room for refinement and optimisation. The benefits of a centralised platform have been far-reaching. Armed with measurable metrics, leaders are able to continuously refine or shift their approach from speed to efficiency or better forecasting.

Another powerful outcome from the new centralised system is the ability to validate assumptions about time-consuming tasks and to move beyond developer productivity to measure the efficiency of shipping products to market.

"We found that while we were effective at executing smaller, innovative projects, we struggled with large-scale, multi-product initiatives. Identifying this allowed us to have strategic discussions at a leadership level about refining our product development process for speed."

Hosanna believes that the most important consideration when driving change is always to lead with business challenges or goals first to avoid being, as she describes it, "a hammer looking for a nail". This approach, she believes, ensures traction particularly in large-scale transformations. Hosanna believes that hiring great people can help organisations to hone the vision and optimise the process, but if there aren't clear outcomes for them, they are being set up for failure. Unsurprisingly therefore, she says that if she had access to an unlimited budget, she would choose to invest it in processes first.

"Oftentimes, processes get a bad rep because they are an afterthought or bogged down by organisational debt. Invest time up-front to be clear on outcomes and instrument your process with success metrics so you'll know if you've got it right."

Technology also plays a role but it can be a distraction and must be fit for purpose, and the tools aligned with business needs, and the long-term costs considered.

"Too often, I've also seen leaders invest in the latest technology, at great opportunity cost, without a clear value proposition in mind."

Spotify has invested in automation "where it makes sense", particularly for repeatable processes, but as their processes are constantly evolving, they tend to avoid large-scale automation that might become too costly to maintain. Instead, the focus is on incremental improvements that provide ongoing efficiency gains. Hosanna takes a very optimistic view of developments like AI and the impact these tools can have on people's roles.

"AI can lower the bar to entry for innovators, democratising and accelerating the technology learning curve. Now employees with other forms of expertise like compliance, security, etc don't have to also be technical experts. They can combine their expertise with AI to discover new approaches to our biggest technical and security challenges. Those who are investing in learning with AI, especially non-technical ones, will be the ones leading the vanguard of the next technology innovation boom."

DAN JONES

Senior Security Advisor, Tanium and formerly Service Owner (Defensive Cyber Operations), UK Ministry of Defence

"It all goes back to leadership, ways of working and culture. None of this is technology-based yet, but you have to have the technology in order to be able to realise that vision. But without the right people working in the right way, your technology is left in a sort of stagnant state."

"Imagine how many of the world's problems we could solve if we got the right people in the right room working in the right way."

There's no doubt in Dan's mind that 'people', or more specifically 'leadership and culture', are the most essential elements of cybersecurity success.

"Cybersecurity is a people problem that's dressed up in technology. Prioritise getting the right people because they will help me figure out the right way of working with whatever technology I've got my hands on at that time so I can exploit it better."

Dan's pride in the diverse team he built during his eight years leading the service development delivery of defensive cyber operations for the UK armed forces is plain to see.

"Diversity was the answer to all of my questions, problems and prayers because I had a brilliant set of people that wanted to work and come in to make a difference, and they came from all kinds of walks, backgrounds, life experiences and all types of genders."

Dan believes that strong, visionary leadership in cybersecurity is essential. Leaders need to be able to understand the challenges and risks, and to be able to communicate effectively between the IT and non-IT aspects of the organisation. They need to have the knowledge and skills to understand the technology and the challenges that the people working with that technology face daily.

"It all goes back to leadership, ways of working and culture. None of this is technology-based yet, but you have to have the technology in order to be able to realise that vision. But without the right people working in the right way, your technology is left in a sort of stagnant state."

He highlights the fact that as every organisation is different, "there's not a 'one size fits all' for your people, process and technology conundrum". He also explains that when considering the impact of people and culture, leaders should also reflect on how their culture extends to their suppliers and partners in that space.

Dan views the resistance to change that stems from fears about the impact of AI on jobs as more of a cultural issue than a factual one. Indeed he believes there is enough demand for IT skills to keep people employed even with AI entering the industry.

People are resistant to change, he argues, because they are comfortable with what they're doing. This reliance on entrenched procedures or legacy ways of working can impede the successful adoption of AI, so strong leaders and visionaries will be needed to guide people through these changes.

People will need to be upskilled and reskilled into roles that require human intellect for decision making. Dan argues that this can be achieved by automating tasks that computers can handle and allowing people to focus on monitoring and decision making.

"To have strong cybersecurity foundations, you need to have good patch management efficacy and, at the moment, that is predominantly a manual process with loads of checks and balances in place. We need to move people to a point where we're going to let the computers run it to a degree or to a set of parameters that a company is happy with in terms of how quickly those updates come through, and move people to a point where they're looking to intervene to stop an update happening when there are indicators."

Dan paints a picture of an ideal scenario where, with the right leadership mindset, tools and ways of working, teams can be proactive rather than reactive to threats.

"When I was working in the Ministry of Defence, I wanted to enable my people to fight back. I didn't want them to be on the back foot having to react to things all the time. I wanted to be able to put them in a position where they could get on top of things before there was a problem."

MATTHEW HARRIET RANDALL

Head of Software Development, Automotive company

"I aim to raise people up so they can be the best they can be and deliver transformative technology."

Matthew Harriet joined the iconic luxury car brand 17 years ago, starting work as a junior developer straight out of university with a degree in aeronautical engineering. In that time, Matthew Harriet has witnessed a lot of changes in “the way things are done” with automation replacing a lot of manual tasks and, in one example, reducing the length of time taken to complete a process from three weeks to three days.

Although their background is rooted in technology rather than management, their greatest aspiration has always been to help others achieve greatness.

“I aim to raise people up so they can be the best they can be and deliver transformative technology.”

Matthew Harriet values the importance of a diverse team and believes that having people doing their best leads to the best results. And despite having a role where they/them champions technology-driven innovation, they/them believes you cannot overlook the impact of people on the likely success of a technology implementation.

“Without good people, it’s hard to establish effective processes, and without those, the technology won't be as effective. Technology itself is less of a stumbling block today. It's more about having the right people to determine the best way forward.”

In Matthew Harriet’s experience over the past decade, technology is no longer the main obstacle in most transformation projects. The bigger challenge, they believe, is choosing the right technology for the specific need, particularly for new organisations faced with an overwhelming number of options. The starting point, they say, must be understanding the problem you’re trying to solve, rather than focusing on the tool itself.

“Don’t implement a new technology just because it’s there. You want to be looking at what problem or what process you’re trying to either improve or get around that a technology or a new tool will achieve. So, no matter which way round, you're not implementing technology for the sake of it. Yes, it may be great and you may see some initial uptake. But without clear goals from the start, it won’t have the longevity you need. At the end of it, you should be able to say, “yes we achieved what we set out to do, or no we didn’t.”

Overcoming resistance requires showing people the benefits. Matthew Harriet acknowledges that change can be difficult but once people understand how it helps them, they are far more likely to embrace it.

JASON BRADLEY
Chief Digital & Data Officer,
NHS Digital

"Skilled staff will assess existing processes, identify suitable solutions and implement them effectively. The NHS has a history of digitising paper-based processes without optimising them for technology which limits efficiency gains. Investing in people ensures that technology is deployed in a way that maximises its benefits."

It's clear from just a short conversation with Jason that he's driven by a powerful mission; to ensure the successful delivery of services for patients and service users within the NHS. Indeed, when our discussion moved to the subject of Jason's aspirations and ambitions for his role, he shared that he wanted to deliver "the best technology, processes and data to support our staff and patients, ensuring we provide the highest quality digital and data services and the best working conditions for our staff".

As Chief Digital and Data Officer, with a seat on the board, security is an important part of his remit. He uses this voice to drive compliance with NHS minimum standards for cybersecurity and data governance, and to embed security ownership at all levels of the organisation. But, as the greatest vulnerability for the NHS comes from third-party suppliers, ensuring departments address these risks is Jason's biggest priority and he says that "ensuring their security is as strong as ours is a critical challenge".

It will come as no surprise that Jason's ambition and capabilities are hindered by financial constraints and resource limitations. When it comes to technology investments, Jason is mindful that the onus is always on tackling NHS business challenges such as productivity, safety and engagement with patients and service users. But investments in maintaining and improving the NHS infrastructure including cybersecurity are also key. Innovation is also an important driver and they are exploring emerging technologies such as AI to assess their potential benefits for service delivery.

The team recently rolled out the integration of sepsis identification into their electronic patient record system. As Jason explains,

"Sepsis is a life-threatening condition that requires immediate action. We are deploying decision-support tools into our system to help clinical teams identify potential cases early, automate test ordering and track performance in real-time and over time. This initiative enhances patient safety and supports more efficient clinical decision-making."

Technology clearly plays an important role in enabling innovations like this to happen. However, if systems and tools can't talk to each other or exchange information, collaboration and innovation will be impossible to achieve.

"We operate multiple systems within and outside our organisation but suppliers in the NHS ecosystem often provide poor interoperability and APIs. Clinicians need seamless access to patient data without duplicating the entry or missing critical information. Achieving an open, connected system architecture will be one of our biggest challenges in the coming years."

Ultimately though, in the NHS, people come first, and if Jason could give his people one gift it would be the time to innovate and develop new capabilities.

"Skilled staff will assess existing processes, identify suitable solutions and implement them effectively. The NHS has a history of digitising paper-based processes without optimising them for technology which limits efficiency gains. Investing in people ensures that technology is deployed in a way that maximises its benefits."

STUART SEYMOUR

Group CISO and CSO, Group Security, Virgin Media O2

"Smart, well-trained individuals will write processes, analyse lessons learned, procure the right technology, run the technology, and improve and tune the technology. The great mistake in our industry is thinking that a tool will be the silver bullet. It's not. It's the combination of all three."

Stuart says that he'd always aspired to become a Chief Information Security Officer, and now that he has achieved his ambition, his greatest aim is to develop his people so that they can be their best selves. He believes that people can get a bad rap in the cybersecurity world and that the perception that "people are the weakest link" is widespread. However, Stuart strongly disputes this opinion and instead views people as a crucial part of development. Indeed, he says, "Machines and AI cannot analyse nuance the way humans can.".

For Stuart, the greatest challenge in his role is not just managing people but ensuring that they are supported, valued and empowered to make a difference. It is here where Stuart finds the greatest reward and satisfaction from his role and feels he can leave a lasting legacy.

"My proudest accomplishments are not the awards I've won, but the people I've mentored who have gone on to achieve great things—whether it's stepping into my former roles or advancing their careers in unexpected ways."

AI and automation play an important role in ensuring Virgin Media O2 is secure and resilient; removing mundane, energy-draining tasks such as moving spreadsheets or handling repetitive security tasks. By automating these processes, Stuart's analysts are freed up to focus on more engaging activities like threat hunting, malware analysis and professional development.

So what type of skills does Stuart look for in his people to thrive in this environment? First and foremost he prioritises curiosity.

"I hire people who take apart toasters just to understand how they work. Curiosity drives innovation in cybersecurity."

Collaboration skills are also important to Stuart so he seeks out people who put the team first and thrive in a cooperative environment. A willingness to learn and to continuously improve and innovate is also invaluable. In addition he believes that people who resist change often take comfort from established legacy processes that can hold back modern practices and slow innovation. Stuart stresses the importance of challenging the 'we've always done it this way' mentality, if an organisation is to be able to move forward.

Armed with an unlimited budget, Stuart would choose to invest in people over process and technology every time. Stuart would also prioritise training after hiring, and only then focus on processes and technology.

"Smart, well-trained individuals will write processes, analyse lessons learned, procure the right technology, run the technology, and improve and tune the technology. The great mistake in our industry is thinking that a tool will be the silver bullet. It's not. It's the combination of all three."

Stuart believes that leaders should look beyond their traditional organisational boundaries to achieve their goals.

"Collaboration amplifies our collective strength. Sharing intelligence, incident responses and lessons learned enable everyone to be more prepared. Some industries are more open than others, but in cybersecurity, transparency benefits everyone. The old saying applies: "If you want to go fast, go alone. If you want to go far, go together."

JULIE MCCOMBIE

Head of IT,
Diabetes UK

"Employees are naturally resistant to change especially when they've been using the same systems for over 14 years. They tend to revert to familiar ways of working even with guidance. Breaking these habits requires strong sponsorship from leadership, a comprehensive adoption roadmap and clear organisation-wide communication."

Julie joined Diabetes UK as Head of IT over six years ago after decades of working on embracing and applying innovative technologies across a number of sectors. Her focus is to overhaul its technology function and describes her role as primarily "introducing and managing transformational change". When Julie joined the charity, many of the existing business processes were not optimised for best practice and data management was a key issue. Rather than trying to untangle all the legacy complexities, Julie's approach was to replace outdated systems entirely and run parallel implementations.

"The systems at Diabetes UK had organically grown over time which is quite common in smaller charities. As these organisations expand, their systems grow with them but the level of maturity in IT processes often doesn't keep pace. This can lead to inefficiencies particularly in system configuration, security and data management. It's often more cost effective and efficient to start fresh than to attempt to fix a system that has become too convoluted."

Before Julie could undertake any of the changes the organisation needed, she first needed to build strong security foundations and enhance IT maturity, and to this end, she transitioned to a Cloud First operating model. .

"We initially built a new, secure tenancy from scratch using the latest Microsoft tools ensuring a solid foundation for all future digital transformation projects, followed by a migration of all servers to Azure. This shift resulted in significant operational cost savings which then allowed us to invest in new initiatives."

Like many organisations, Diabetes UK had data silos and data quality issues that were created when their legacy systems had been modified so extensively they became difficult to maintain. Rather than trying to work around these outdated systems, Diabetes UK decided to move to a new CRM system and introduce a modern data platform, compatible with Fabric, Microsoft's AI insights platform.

"We're leveraging machine learning for data transformation, deduplication, merging and validation. One of our more ambitious projects was developing a Power App tool to handle data exceptions within the business. Our goal was to push data responsibility back to our colleagues rather than having it sit with the data team. Machine learning helps us clean and merge data but we need business teams to validate exceptions."

Julie concedes that the implementation process has been challenging and has taken longer than they expected. But now that the technology is ready for moving into service delivery, Julie outlines an even bigger challenge; implementing people and process change.

"Employees are naturally resistant to change especially when they've been using the same systems for over 14 years. They tend to revert to familiar ways of working even with guidance. Breaking these habits requires strong sponsorship from leadership, a comprehensive adoption roadmap and clear organisation-wide communication."

Automation and AI serve a higher purpose at Diabetes UK than simply delivering cost savings and efficiencies. The charity is passionate about using technology to free people up for higher-level work that furthers their research and advocacy efforts.

"Science is well on the way to identifying markers for Type 1 diabetes in children which means we can predict who is likely to develop the condition later in life. The next step is ensuring this knowledge is embedded throughout the NHS so testing can be widely implemented and clear treatment pathways can be established. By automating routine tasks, our colleagues can focus on embedding these critical advancements that will have a real impact on people's lives."

JIM GREEN

Technical Director, AI & Data Team Lead, AtkinsRéalis

"It's about prediction. It's about classification and once you understand the kind of building blocks of what AI can actually achieve, it's a lot less scary. Humans are fantastic at multitasking and juggling all sorts of complex problems while AI at the moment is not really good at that."

With a background running big data programmes in Defence Intelligence, Jim joined engineering consultancy company AtkinsRéalis as a Technical Director. He mainly works with public sector and critical national infrastructure clients where AI is the hot topic of conversation. Jim believes AI's true value currently lies in automating dull, repetitive tasks that humans find tedious. And in an industry where security is so key, in helping to bolster cybersecurity defence.

"When we look at what AI is optimising, it really is back-end efficiencies. It tackles those mundane tasks that humans often find repetitive and dull. Automating these processes is where AI shines. While discussions about generative or general AI and their future potential are exciting, the real impact for me is in eliminating tedious tasks."

Jim feels passionately about how AI automation can push employees up the value chain.

"What I'm excited to achieve is helping get our government organisations to a place where they've got that high threshold already and we can start sprinkling the AI on top so that everyone is performing where they need to perform."

Jim believes that the AI hype cycle peaked last year and has since slowed down, with the focus shifting from flashy features to practical uses and real-world results. From his experience, he believes AI has evolved beyond pilot projects and experimentation to implementation, and this brings with it a whole set of new challenges with integration, scalability and trust. Jim believes that rather than seeing AI as a technology integration programme, it should be approached as a change management initiative with AI being just one piece of the jigsaw. But scaling this to enterprise level is, he admits, very challenging.

"With scalability you need to have the hardware enabled for that and a lot of that is about migrating to the cloud. Significant swathes of the public sector have now moved to cloud, but there's still a challenge with certain kinds of business units doing that migration and building confidence to migrate to cloud from a security perspective."

Trust issues are particularly key in areas of defence and critical national security. Trust in the algorithm is vital but there also needs to be transparency about what 'good' and 'bad' looks like. That requires upskilling your workforce not only in AI skills but also fundamental digital literacy which is still lacking in many organisations.

Jim believes that the biggest pain points in the organisation can be traced back to legacy processes rather than technology.

"The technology is generally pretty simple. I say that you can buy a new server rack or you can migrate to cloud, and there are some great cloud providers available and they're secured to the appropriate levels. That's all achievable. The people and the processes are the bit where it gets really interesting to my mind, particularly when you start to scale."

Jim also highlights the dangers of outdated workflows and an underlying reticence to change that's holding back the inculcation of AI at scale. Risk aversion is also high among the defence and critical national infrastructure community.

"All change is scary in some shape or form because it's moving into an unknown system. It's about education and that can be done in a really light, informal manner."

Jim recommends spending time with people and breaking down AI into bite-sized, understandable chunks as this helps them understand where they fit in the AI value chain.

"It's about prediction. It's about classification and once you understand the kind of building blocks of what AI can actually achieve, it's a lot less scary. Humans are fantastic at multitasking and juggling all sorts of complex problems while AI at the moment is not really good at that."

When it comes to decisions on purchasing new technology, Jim cautions, "Why is 'new' always better when the pain of migrating from one software package to another at enterprise level can be so significant. Indeed he advises that leaders ask themselves, is the benefit worth it or are you just adding complexity?".

"Often, organisations haven't integrated the tool properly, so they try and move software and think that will solve the problem, but that's not the problem. The problems come back time and time again to the people and the processes, and the software is just the relatively static, simple piece."

DAMIEN BENAZET

Area Vice President - Customer Success, Tanium and formerly Head of End-User Computing, French CAC40 company

"You should use these highly skilled people for something that brings more value to your business, for inventing solutions and finding innovative ways of serving your business."

A lack of reliable data is the biggest challenge facing IT leaders in 2025 according to Damien Benazet, Area Vice President - Customer Success at Tanium, and formerly Head of End-User Computing at a Tanium customer. In fact, he argues that this is the reason why so many IT projects are currently stalled, regardless of whether these initiatives have a cybersecurity or operational focus. People and process matter too but both are pointless, he believes, if the underlying tools don't supply up-to-date and reliable data.

Complexity is another issue that is a major concern for IT leaders; the all-too-common result of an accumulation of tools in the IT estate. He describes a typical scenario that can hamper both the efficient running of the business and the ability to pinpoint responsibility for incidents or disruptions.

"A company's IT estate has become very complex over the years due to their "one problem, one tool" approach. This has resulted in numerous tools and dozens of product owners who don't communicate with each other. When an incident occurs in production, it's difficult to determine who is responsible due to this fragmented structure."

Freed from the constraints of data silos and unreliable data, he argues that organisations would be able to maximise efficiencies and cost savings, and achieve more with less people and resources. In this world, tools would automate tasks like patching, inventory and vulnerability remediation which are currently being done by highly skilled engineers. This will free up those engineers for higher-value tasks like innovation, finding new ways to serve the business with IT and improving the digital employee experience.

"You should use these highly skilled people for something that brings more value to your business, for inventing solutions and finding innovative ways of serving your business."

DUNCAN HAYES

Head of Cyber Defence,
Hargreaves Lansdown

"The best security tools mean nothing without skilled, well-supported professionals to operate them."

It's not enough to have a compliance framework and hope that this will be enough to keep your organisation safe, according to Duncan Hayes, Head of Cyber Defence at Hargreaves Lansdown. Instead, he relies on a methodology called threat-informed defence that focuses on measuring security effectiveness rather than just implementing compliance controls. Duncan and his team ensure that those controls are effective at stopping the threats they face.

"Compliance alone isn't security. Did you know that all of the top 10 ransomware attacks in the UK last year happened to companies that were ISO27001 compliant?"

Duncan's approach uses threat intelligence to track threat actors targeting financial services and the MITRE ATT&CK framework to analyse attack methods. His team works proactively to test his organisation's defences by simulating real-world attacks with an internal red team. The team conducts adversary emulation, replicating the techniques, tactics and procedures (TTPs) of real attackers to validate and strengthen their controls. Beyond simply running automated scans, they're able to simulate how an actual attacker would compromise their environment.

"We don't just assume a security control works, we actively test if it can detect and prevent threats like ransomware."

The team also analyses how well their security operations centre (SOC) handles alerts.

"I have a rule for SOC efficiency and efficacy of "no messing around". I don't want my team to be dealing with many false positives so our detection engineering ensures that we optimise our alerting so the analysts deal with actual events, instead of just noise."

Duncan acknowledges that cybersecurity is a tech-heavy field but asserts that technology alone doesn't solve problems, rather people do.

"The best security tools mean nothing without skilled, well-supported professionals to operate them."

The mental health of his team is a priority for Duncan, and he believes automation can play a key role in reducing the burden of manual, repetitive tasks, and help analysts stay engaged and curious. Significantly for businesses, Duncan believes that many breaches happen because analysts don't recognise anomalies due to alert fatigue or lack of context.

"Security professionals enjoy their jobs when they're solving interesting problems, not sifting through endless alerts. Our goal is to use AI and automation to enhance their efficiency, while keeping their roles engaging. AI can help contextualise alerts,

filter out false positives and provide actionable intelligence. This allows our analysts to focus on investigations that require human intuition and lateral thinking."

So far, the response to automation from staff has been positive. However, Duncan maintains that it's important to strike the right balance, using AI for efficiency whilst ensuring human expertise remains at the centre of decision making. Indeed, as he explains, "our analysts make the final judgment calls".

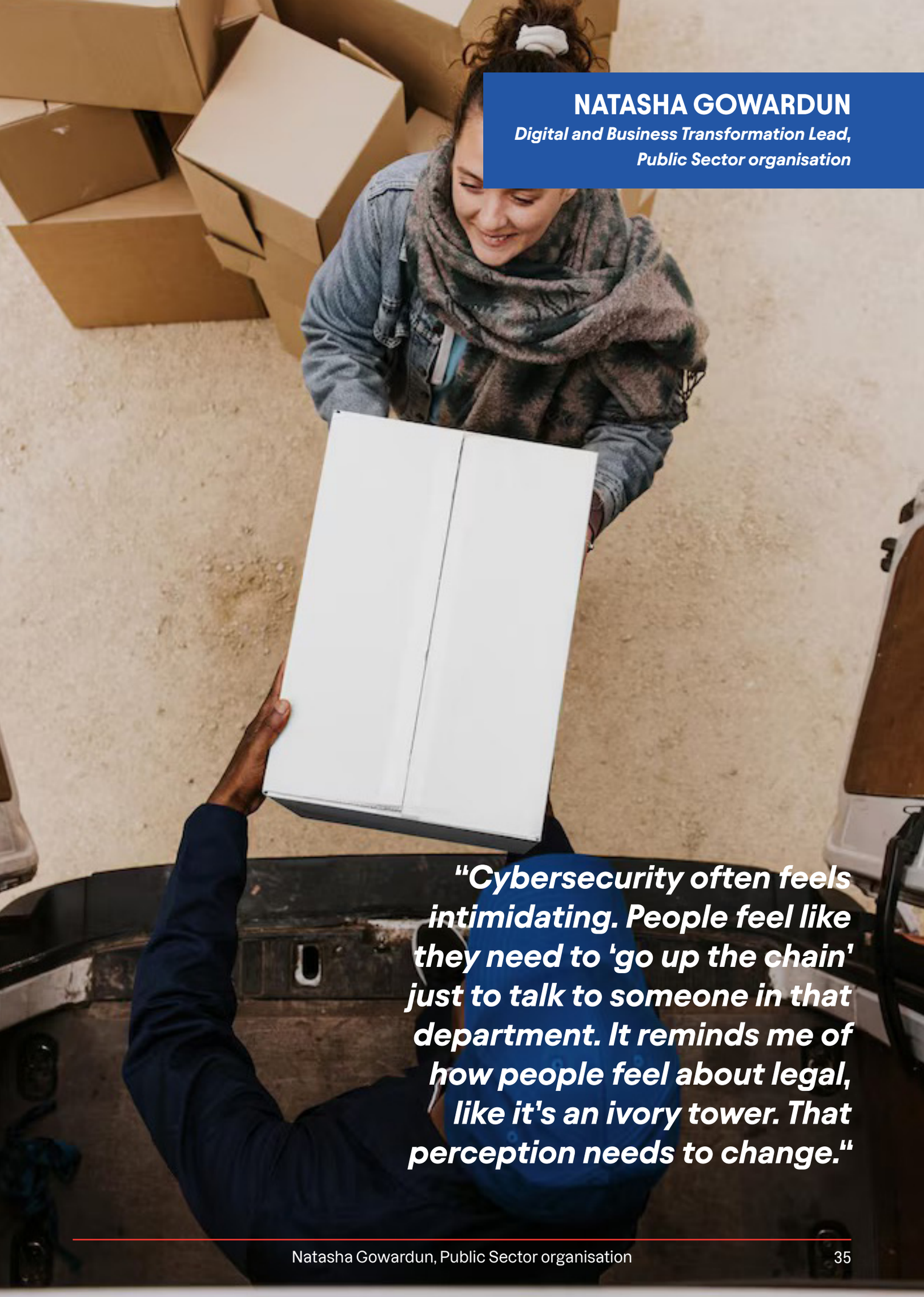
In the two years since Duncan joined the company, he's made a lot of progress on his goals. And, though there's more to do, he's very clear on what success would look like.

"Ideally, I'd want a security operations centre (SOC) where every alert that comes through is meaningful, false positives are minimal and investigations can be conducted seamlessly in a single console. AI would handle the noise allowing analysts to focus on genuine threats. Ultimately, my goal is to foster a security team that remains engaged, curious and effective in stopping attacks before they cause harm."

Duncan refers to the existence of 'friction' several times in conversation. Friction is the organisation's resistance or operational drag on processes that causes them to be inefficient. Friction is present in every company, large or small but the key is to identify where this is present and not just to do things 'because we've always done it this way'. As Duncan explains, "What worked in a small team, like asking everyone around the table for their approval, 'because everyone needs a say', becomes inefficient at scale.".

Crucially, Duncan believes, it's also vital for leaders to understand the skills needed to manage business processes at scale, ensuring that people understand their role in the bigger picture. He firmly believes that most people want to do a good job but they can become disengaged if they feel like their work doesn't matter. Helping them understand how their role fits into the bigger picture and ensuring that the right people are in the right roles is important for success.

"If someone doesn't grasp the purpose of a process, they may not prioritise their work effectively. Over time, processes become bloated and extra steps are added to address issues without reassessing the original goal. To fix this, I focus on stripping processes back to first principles: What are we trying to achieve? How do we do it efficiently while reducing risk and cost?"



NATASHA GOWARDUN

Digital and Business Transformation Lead,
Public Sector organisation

"Cybersecurity often feels intimidating. People feel like they need to 'go up the chain' just to talk to someone in that department. It reminds me of how people feel about legal, like it's an ivory tower. That perception needs to change."

"If people feel safe, if they know the end goal, if they're included and respected, they'll give you everything."

Natasha is a seasoned transformation lead, specialising in project delivery, PMO leadership and technology operations. Most of her background has been in retail technology and her experience has led her to conclude that, "transformation is never really done and that as technology evolves so do the needs of businesses".

Her aspiration is to come up with a set of fundamental solutions that address what she sees as the "recurring issues" in retail technology, and she firmly believes success comes down to getting the basics right.

"To create secure and resilient operations, my fundamentals would include strong communication, stakeholder engagement, clear planning and accountability, and a shared understanding of roles and responsibilities."

Natasha believes that the word 'transformation' has become something of a buzzword of late, but that real transformation is messy, painful and complex. In her eyes, people always come first, whether that's a strong, resilient leader or just the right team in place who'll shape the right processes. She's witnessed first-hand the consequences of poor leadership and wrong hires in her recent role and believes, "if you bring in the right people with the right experience, everything else can follow.".

Engagement with the cybersecurity and reliance strategy can be tricky to achieve especially if the CISO function is new. But this is where she believes robust processes come into play. Furthermore, she thinks the function needs to work on the perception that it is "some mysterious or isolated department".

"Cybersecurity often feels intimidating. People feel like they need to 'go up the chain' just to talk to someone in that department. It reminds me of how people feel about legal, like it's an ivory tower. That perception needs to change."

Natasha describes their journey to automation as "painful" and thinks they still have a long way to go, partly because the organisation operates in a very traditional, 1980s-style waterfall model.

"About a year ago, our tech leaders recognised that this way of working just wasn't sustainable. Every piece of work had to go through stage-gated approval processes which meant if you were building something substantial, it could take forever just to get it signed off. Not necessarily because of the teams doing the work but because of the sheer number of approvers involved.

That's one of our biggest problems: too many people needing to know everything but also being too afraid to approve anything."

The solution was a shift to Agile, a change that was done gradually through tweaks to avoid unsettling the team. They also started using Jira and Confluence to track progress properly and that's when they began to see real value through automation, quality improvements and reliable reporting.

"Reports became our truth. Nobody could argue with the data. That visibility helped us push even further and we began training the teams too. We had industry experts come in and help overhaul our approach. It brought credibility, motivation and people actually started to enjoy the process. We're still on that journey, but once the graphs started going up and people saw the momentum building, it created a positive culture."

Natasha feels passionately about the need to improve psychological safety and trust. Leadership plays a huge role in this and if the leadership team isn't aligned or they are working in silos using different processes, it falls apart. She argues that transparency with everyone, not just leadership, is also vital to take people on the change journey.

"One tool we've used is anonymous Slido Q&As during sessions. You get the brutal truth sometimes, really brutal! But if you're going to give people a platform, you've got to be ready to hear what they have to say, and you can't ignore it."

ANONYMOUS

Chief Risk Officer, Media and broadcasting company

"The focus should be on adapting to change. Automation often addresses today's problems but we need people to anticipate how risks and technologies evolve."

As Chief Risk Officer at a global media and broadcasting company, he oversees all major risk programmes in the organisation including their enterprise risk framework. He also has responsibilities covering resilience and business continuity which are directly related to technology. Operating in a highly competitive and fast-moving market, he values the ability to understand how the environment is evolving and the ability to adapt quickly to changing circumstances.

"The focus should be on adapting to change. Automation often addresses today's problems but we need people to anticipate how risks and technologies evolve."

His greatest aspiration is to ensure that business decisions are made with a risk-based approach.

"I want risk management to be at the core of our decision making so we take the right risks and fully understand what we're exposing ourselves to."

He argues that many organisations still don't have a strong culture of risk-based decision making. There's often an "optimism bias" where people assume everything will go smoothly rather than considering what could go wrong and this cultural challenge makes it difficult to integrate risk thinking into everyday business operations.

Given the opportunity, he would like to create a dedicated AI team to explore both the opportunities and risks AI presents. Currently, responsibility for AI sits across a number of roles but he believes that having specialists would be a more effective approach. He would also have a dedicated external liaison role to stay connected with industry developments and ensure they're learning from and sharing best practices with other organisations. He believes their cybersecurity capabilities are strong but admits that there's room for improvement in resilience. From his perspective, the key is understanding resilience at a business-wide level rather than just at the system level. In addition, to focus on end-to-end processes and what the business truly requires from resilience planning, rather than just individual system uptime.

"I think there is a lot more to still do on resilience and actually understanding end-to-end processes as opposed to the resilience of individual systems, platforms or tools. So understanding what the business really needs from resilience as opposed to what an individual systems' owner needs from it."

He concedes that silos still exist between IT security and IT operations, though they work hard in the organisation to minimise them.

"Both functions are extremely busy which means teams don't always consider the other's perspective. While the situation has improved, there's still room for better collaboration and integration between IT security and IT operations."

HARPREET SINGH SETHI

Global Head of Technology (UFS), Unilever

"By automating repetitive tasks, we free up valuable time for our team to focus on strategic and creative work. AI also helps us leverage advanced analytics and predictive capabilities, allowing us to make data-driven decisions rather than relying on opinions."

Harpreet has been Global Head of Technology at UNI Food Solutions, part of the Foods Business Group at Unilever, for the last nine years. He leads a global team responsible for converting business needs into technology solutions across over 76 markets. Over the past few years, he's been focused on digital transformation, leveraging technology, data and AI to accelerate business growth.

Historically, the team used technology and data to drive business growth. But now, with the rise of AI and its accessibility at lower costs, they're exploring new ways to accelerate business transformation.

"By automating repetitive tasks, we free up valuable time for our team to focus on strategic and creative work. AI also helps us leverage advanced analytics and predictive capabilities, allowing us to make data-driven decisions rather than relying on opinions."

They've been using AI in various ways including, enabling their marketing team to create content at lightning speed for hyper-targeted communication and personalisation, using AI-powered translation tools and developing personalised AI solutions tailored to their industry needs.

Harpreet believes AI is all about automation and helping people do things more efficiently such as automating processes and reducing the burden on their developers and business teams.

"We've integrated GitHub Copilot to help our developers write code faster and more efficiently, leading to better-quality code. Automation, powered by AI, helps us achieve more in less time and enhances our overall efficiency."

When evaluating new tools and technologies, Harpreet advises to focus on two key aspects: Do they empower the business to achieve more? Are they a step forward in terms of innovation and efficiency? He also argues for taking a long-term view of the investment.

"I also consider whether the solution meets not just today's needs but also our future requirements for the next four to five years, or even 10 years, depending on the level of investment."

Technology is central to Unilever's digital transformation journey which has reshaped their business across several key areas including operational excellence, digital experience transformation, e-commerce transformation and data-driven decision making.

"Unilever has been in the B2B food service business for decades. Traditionally, sales representatives would visit restaurants in person, demonstrate products and collect orders manually. We introduced an e-commerce solution allowing restaurants to place orders online eliminating the need for manual visits. It was a huge success and today our e-commerce business is worth over €375 million. Similarly, we were sending around 4 million emails to customers. Today, thanks to technology, we send 27 million highly personalised emails, ensuring our customers receive the right information at the right time. Technology has transformed our business, accelerating growth while enhancing the customer experience."

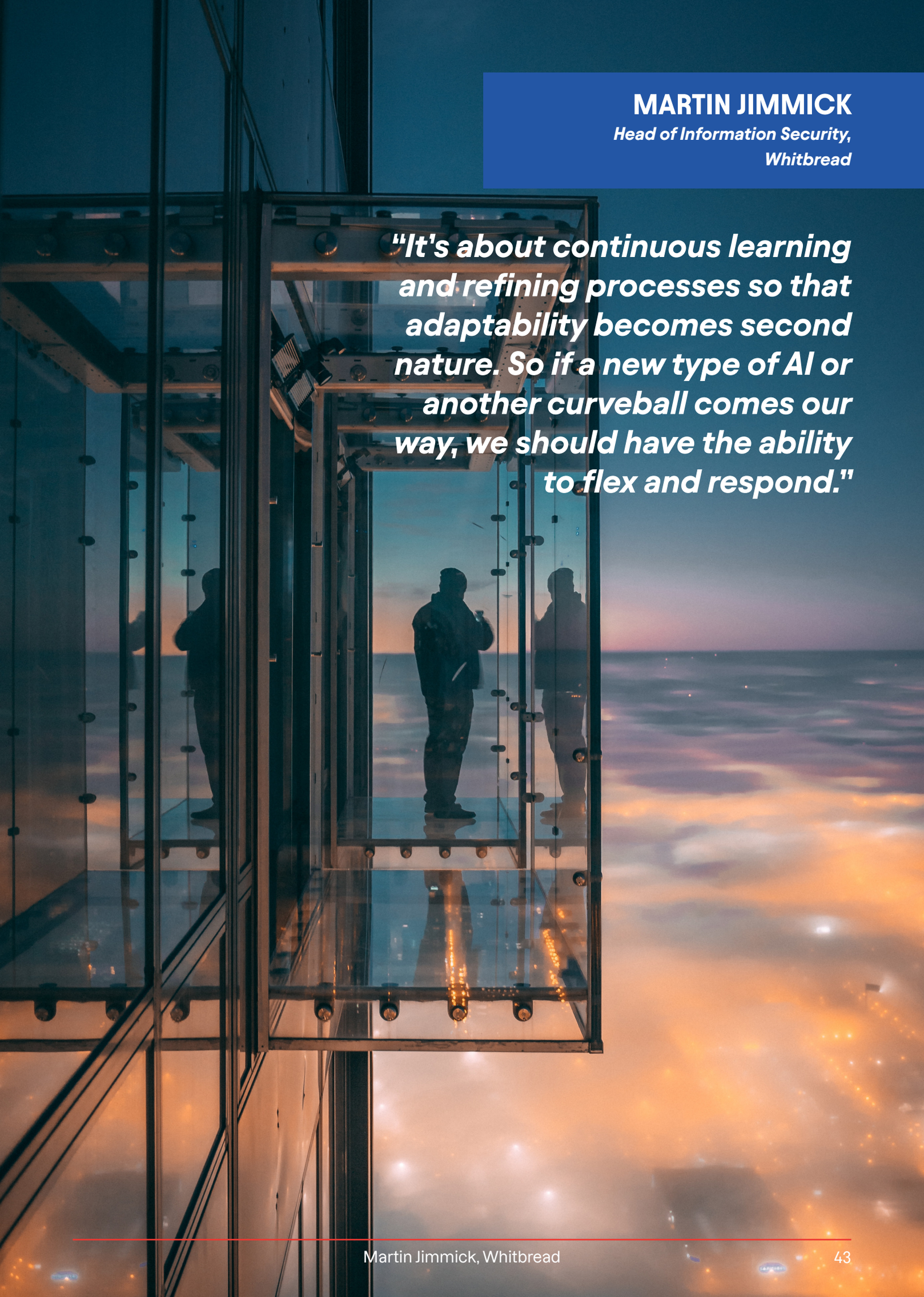
AI and automation are elevating his teams to become more strategic and to innovate faster. By enabling developers to use GitHub Copilot and other AI-powered tools, they've significantly reduced time-to-market for delivering solutions allowing them to focus on more strategic, high-value projects.

Harpreet argues that technology alone doesn't drive real business change. To fully operationalise a solution requires the right tooling, the right skill set and the right mindset.

"Over the years, I've realised that great ideas need both wings to fly and landing gear to succeed. This means investing heavily in change management, upskilling resources and business awareness to ensure our stakeholders can effectively use new technologies."

Despite Harpreet's fervour for technology, he believes you can't just invest in technology without the right people and processes to drive it, describing it as, "trying to run a three-wheeled vehicle without one of its wheels".

However, if forced to choose, he would prioritise spending on technology to build powerful solutions that empower the business. Next, he would invest in people to ensure they have the right talent and skill development, followed by processes to make sure they can scale and sustain innovation.



MARTIN JIMMICK
Head of Information Security, Whitbread

"It's about continuous learning and refining processes so that adaptability becomes second nature. So if a new type of AI or another curveball comes our way, we should have the ability to flex and respond."

Martin leads a team responsible for commercial and customer-facing security at the leading hospitality business, Whitbread. Unsurprisingly, given the nature of the industry and the brands it runs, a major focus of the role is protecting customer data from "disruptive attacks" or attempts to steal information, and ransomware is becoming a more common threat.

Cybersecurity operations at Whitbread are divided into specialised teams with a security operations team, a governance, risk and compliance (GRC) team and, more recently, business engagement teams. In addition to Martin's external-facing team, another team handles internal, colleague-facing security. This dual structure ensures comprehensive coverage but the overlap between teams can create communication challenges that require careful monitoring.

"The networking infrastructure in our hotels falls under core technology security but customer-facing elements like self-service kiosks or digital restaurant bookings are managed by the commercial side. Overlaps like these require careful coordination to ensure thorough security checks and alignment."

Conflicts have been known to arise between security and operational priorities when operational teams want to launch initiatives quickly, making it challenging to implement the right security controls. So balancing speed with security is an ongoing effort, and Martin believes that ensuring both sides collaborate effectively is key.

"We focus on fostering collaboration and communication. Cross-functional assurance efforts ensure that initiatives undergo comprehensive security reviews. Regular alignment meetings, joint planning sessions and clear accountability also help reduce friction. By promoting a shared understanding of security priorities, we can navigate challenges more effectively."

With business objectives and market demands moving at such a rapid pace, Martin sees process modernisation as a core priority as he finds that legacy processes can significantly impact business agility.

"Traditional processes often require a lot of manual effort and human intervention to move tasks forward. Even with modern service desk software and ticketing platforms providing better control and visibility, we still experience friction."

Martin believes that implementing AI and further automation will help them align operational speed with business goals, significantly reducing friction and speeding up initiatives. But while he recognises AI's potential, he is also cautious about the "significant risks" surrounding AI and warns that many people are unaware of how these risks manifest. He says,

"Traditional phishing emails are evolving and even something as simple as a barcode can pose security threats. There's a growing need to educate individuals, providing them with a broader understanding of these changing threats."

Martin stresses that implementing governance and safeguards is vital but that, with clear guardrails, AI technologies can be introduced responsibly and effectively.

When prompted to describe his aspirations at Whitbread, Martin explains why defining success in such a fast-moving and disruptive landscape as cybersecurity can be so challenging. As he puts it, "What we define as success today could change tomorrow.". Unsurprisingly, enabling adaptability is his goal and ensuring that people, processes and technology are aligned to allow for quicker and more effective responses.

"Real success, to me, would involve building resilience, fostering a knowledgeable workforce and remaining agile in the face of evolving threats. That adaptability and readiness would be a true mark of success in my role. Flexibility is key. I believe the vision should be about creating security strategies and teams that are adaptable enough to deal with that kind of disruption, react to it and grow that muscle memory."

This muscle memory, he explains, results in a team that behaves like a well-oiled machine; responding instinctively to challenges as they arise because they've built that experience.

"It's about continuous learning and refining processes so that adaptability becomes second nature. So if a new type of AI or another curveball comes our way, we should have the ability to flex and respond."

GUILLAUME LENGLET

Director of Infrastructure and Production, Xelians

"I evaluate each technology based on its ability to simplify operations, reduce risks and free up time for my teams."

Guillaume Lenglet is Director of Infrastructure and Production at Xelians. Their primary focus is the preservation of paper archives. Today they store and manage digital data in data centres. He manages several teams including an infrastructure team that automates the delivery of virtual machines. They focus on preserving data integrity and reducing the risks of data corruption or theft.

Guillaume's main business priorities are security, agility and efficiency, and he ensures that these are at the forefront of any decisions on investing in new tools or technologies.

"I evaluate each technology based on its ability to simplify operations, reduce risks and free up time for my teams."

Guillaume acknowledges that AI and automation are transforming the cybersecurity world but he argues that this should be viewed as an opportunity, not a threat.

"It allows us to anticipate threats, detect anomalies faster and improve responsiveness. However this requires mastery of the tools and a clear ethical framework."

Guillaume concedes that there are some technological challenges associated with adopting AI, machine learning and automation. However the main challenge is integration into sometimes outdated systems. He also highlights a need to focus on training of teams and managing expectations. We also need to secure the usage especially regarding the data used and automated decisions.

So far his team has automated the OS updates, compliance checks and some deployments. This has reduced the operational workload and allowed them to focus efforts on high-value tasks.

Guillaume explains that if they could achieve full visibility of their endpoints, they would be able to shift from a reactive to a proactive posture. It would also enhance their ability to detect anomalies quickly and prioritise remediation actions. The impact of full data accessibility would, he says, be transformational.

"Data is a lever for transformation when properly utilised. It would enable predictive analysis, better resource allocation and more informed decision making. Reliable predictions from our data would allow us to anticipate incidents, smooth out workload peaks, better plan technical evolutions and justify budget decisions based on facts."

His greatest concern about his data is the protection of sensitive data, especially given what he sees as the increasing risks of leaks or breaches. He is also concerned with the quality and reliability of the data used for strategic decisions. He believes that his greatest opportunity from data is to better understand usage and behaviour in order to continuously adapt their IT strategy.

LAUREN WILSON

Senior Leader in Incident Management, Energy company

"Safeguarding our organisations, and in turn the UK, gives us the best chance of securing an increasingly digital and complex world."

Lauren works in a leadership role at the Office of UK CISO, at an energy company. As a critical part of the UK's energy infrastructure, the organisation is highly regulated and has a diverse cybersecurity landscape.

Lauren describes herself as a passionate cybersecurity leader. She has over a decade of experience in cyber defence, predominantly in the public sector, but more recently in critical national infrastructure. Specialising in incident response and cyber resilience, she has led the technical, operational and strategic cyber incident management functions for critical organisations, " building capabilities that not only support during moments of crisis but also strengthen long-term strategic readiness".

What drives her every day is the ongoing battle against the expanding attack surface and an evolving threat landscape. She believes that the biggest challenge facing cybersecurity leaders today is the ability to manage the juggle between operational firefighting and the strategic capacity to horizon scan and embed the maturity uplift activities needed to meet future challenges. She argues that these difficulties can only be met through the intersection of people, process and technology.

Perhaps contrary to expectations, Lauren would prioritise investing in process over people and technology as they provide the strong, foundational guardrails that ensure the organisation remains safe.

"While people can be trained and technology deployed, robust processes ensure both are used effectively, consistently and at scale."

Lauren feels strongly about being part of a wider mission as a cybersecurity leader, to both contribute to a safer cyberspace today and to also strengthen the resilience of organisations for the future.

"Safeguarding our organisations, and in turn the UK, gives us the best chance of securing an increasingly digital and complex world."

Lauren strongly values collaboration between cybersecurity leaders, not only within the organisation but also beyond, and talks of the importance of breaking down silos.

"As individuals, we are guilty of focusing on the 'crocodile nearest the boat', not through ignorance but often the demands of our roles and lives. Creating a psychologically-safe environment is an effective way to take off those blinkers, break down those silos and allow for the vital collaboration needed to succeed."

DR MARK DANIELL
CTO, Prototype Warfare and Disruptive Technology, Aerospace, Defence and Security company

SIMON HARWOOD
UK Strategy & Technology Director Aerospace, Defence and Security company

"It's crucial to foster a mindset open to risk and fast-paced development. Process is also important to support people and ensure they're covered by the organisation. However, large organisations like ours can become process-heavy which isn't as much of an issue for SMEs."

"It's a loop or triangle: people, process and technology are inseparable."

Mark and Simon work together creating new technology products and services for a global industrial group that builds technological capabilities in aerospace, defence and security. It's a company that works beyond the frontiers of innovation so, as you might expect, Mark and Simon's greatest aspiration is to move technologies from development to deployment where customers can experience their value. Their aim is to accelerate the implementation of these technologies and argue the need to shift from a "peacetime development mentality" towards much more urgent development.

Mark describes the synergy between people, process and technology as "all interconnected. Efficient processes, supported by technology, determine how people are utilised.". But both agree that the most important factor is people and culture. Simon explains,

"It's crucial to foster a mindset open to risk and fast-paced development. Process is also important to support people and ensure they're covered by the organisation. However, large organisations like ours can become process-heavy which isn't as much of an issue for SMEs."

Simon also believes that modern practices are being held back by legacy processes and describes the experience of their move to the cloud to illustrate the point.

"Historically, we used traditional file shares and filing systems. However, moving to the cloud requires a completely new process especially from a security standpoint. Security remains essential but the approach has to be different. People used to older systems might not evolve as quickly to new ways of working and, in that sense, legacy processes can definitely hold back productivity."

Mark describes the company in the past as "massively siloed"; geographically spread across the UK, with different business lines and divisions. Many parts of the company were originally separate legal entities that got merged and their IT systems had to be "cobbled together" over time. However, he explains that things are improving and the digital solutions group and IT teams are actively working to address and reduce these silos in the digital era.

As you might expect, there's a high demand for software development and coding skills. However, traditional engineering disciplines are also still very much in demand, for example in firmware, electrical and mechanical engineering. But Simon thinks it's important to think beyond just technical skills, and they're placing more emphasis on aptitude over just qualifications.

"Someone might have a degree in engineering but lack communication skills, and vice versa. So we look for both technical proficiency and those softer, foundational skills like collaboration and leadership."

Mark adds that they need to be more deliberate about not just recruiting for what the business looks like today, but for what it needs to become.

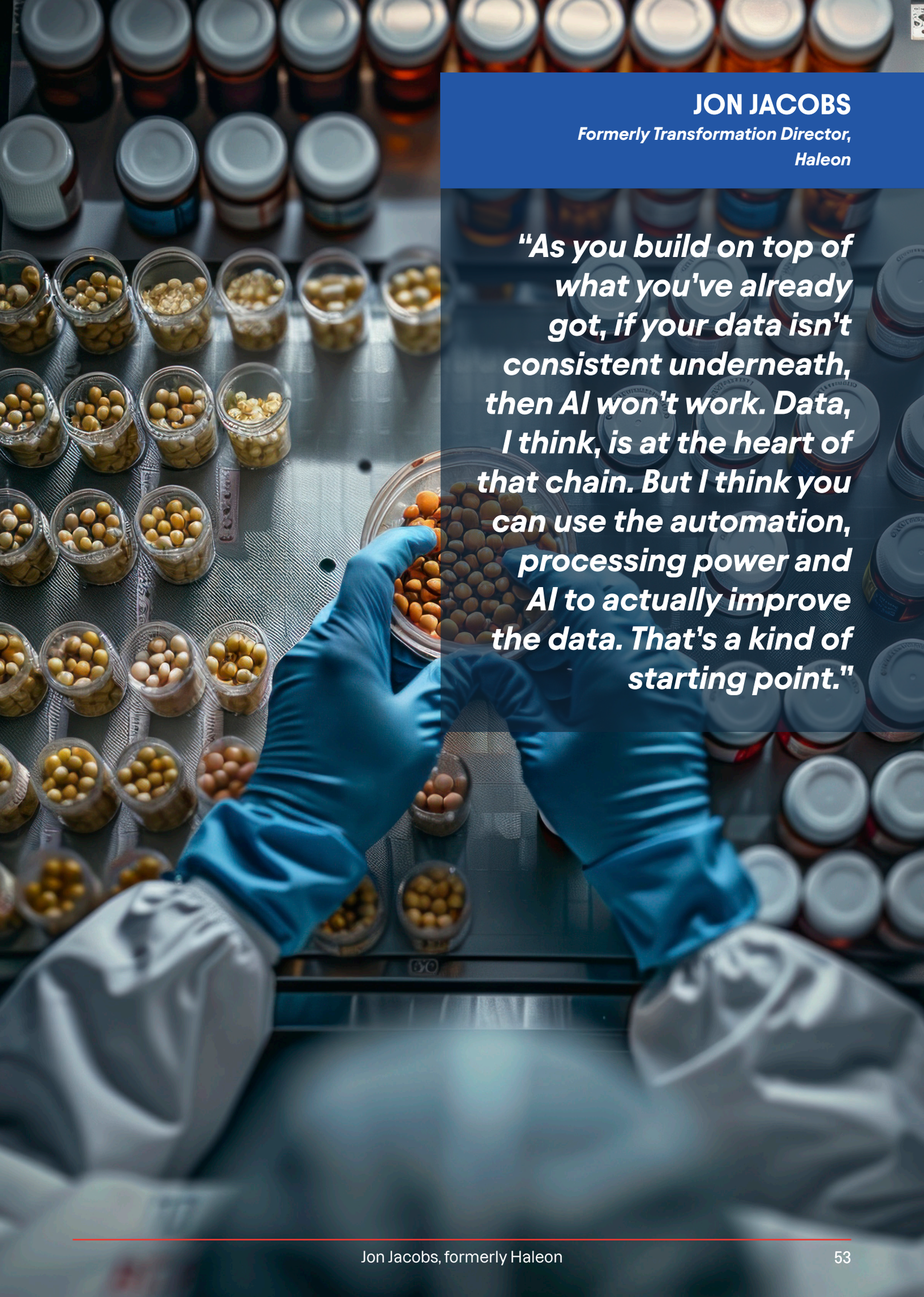
"Take AI and machine learning. We bring in graduates with those skills but then shape them into radar or systems engineers because that's our current structure. Instead, we should let them stay as machine-learning experts and evolve our teams around that. It's about adapting to new skill sets rather than always adapting people into old molds."

Interestingly they make the point that although the most attention is given to the early career pipeline, the bigger issue is actually mid-career retention, with those in the 35 to 45 age range and with 10 to 15 years of experience, and it is here that they see a significant gap.

Mark and Simon agree that the organisation has worked hard to encourage more inclusive hiring, including women and ethnic minorities. However, in doing so, the organisation has sometimes overlooked the existing core demographic, which can also lead to imbalance. Mark maintains that it's all about finding the right balance across the board and the responsibility does not sit solely with employers.

"The real change has to start in primary school, getting girls and underrepresented groups interested in STEM early. If people don't apply to us, we can't hire them."

One of the major recruitment obstacles they face is the restriction on nationalities they can employ, for obvious security reasons, and they struggle to recruit for data-driven roles like data engineers, data architects and data scientists. Furthermore, an inability to compete with other sectors on salary and misconceptions or unfair associations with the oil and gas industry make it harder to attract the best talent.



JON JACOBS

Formerly Transformation Director, Haleon

"As you build on top of what you've already got, if your data isn't consistent underneath, then AI won't work. Data, I think, is at the heart of that chain. But I think you can use the automation, processing power and AI to actually improve the data. That's a kind of starting point."

Jon describes his former role as Transformation Director at global consumer healthcare company Haleon as, “managing teams and solving technical problems at a management and transformation level”.

Transformation is certainly a phrase that many would associate with Haleon following its formation back in 2022 when GSK spun off its consumer healthcare business. Jon led a programme called Process Improvement and Automation, an initiative focused on streamlining the complex processes they had largely inherited from the old company. Jon explains some of the challenges they were facing after having inherited an old, siloed tech stack and his ambition to bring this under control through automation orchestration.

“So many people have so many different tools. Often doing the same things, so linking it and automating it together so it is more efficient and joined up is key. And that's either a new tool replacing free tools or it's putting some automation across something. I think that's actually where AI and, I'd say, orchestration can come in and help. Often we have so many different things going on that are complicated, and that often drives a lot of manual work, but with the power of AI and general orchestration automation, these can be minimised or resolved.”

There are always multiple priorities at any given time so when it comes to considering where to prioritise attention, Jon advises to identify the things that can really make a difference.

“The main driver is cost, and it nearly always is. But we decided that it was not the only driver. We had three drivers; cost efficiency, making things work better and user experience. So we did things in our programme that weren't just about reducing costs. They had to make a difference in the way we worked and simplifying things, and in the end, making the user actually benefit from it. We tried to quantify that. It's not easy but we tried to justify that these things actually improve user experience and make the organisation simpler.”

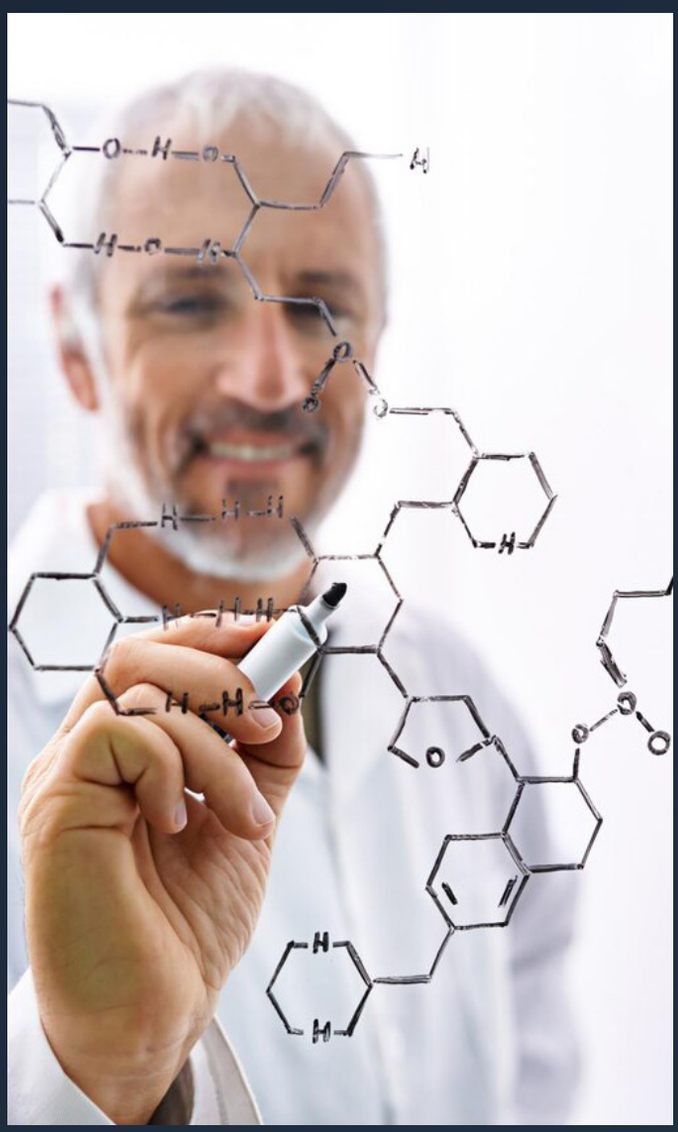
But while Jon views automation as essential, it’s certainly not been an easy task to implement.

"There is so much that doesn't work that well in the tech stack, partly because it's old, partly because it's siloed and partly because it's just in people's brains. There's also the pressure to reduce costs, automate, make things simpler and to actually improve the experience of users. It sounds simple but actually doing it, making it work and stick, and bringing people on that journey is difficult. Someone said to me very recently, the problem isn't the tech, it's the people... if you're changing people's jobs, changing what they're doing, having people do things differently, that's the tough bit as well."

Being able to trust the data is also key and Jon believes the greatest opportunity with data is having the tools that can understand all the different forms of data, to clean it and make it consistent. He's excited about what AI can do for organisations but also warns of the dangers of teams losing confidence in the data and then failing to use it. Jon also stresses the significance of consistent data for effective AI implementation.

"As you build on top of what you've already got, if your data isn't consistent underneath, then AI won't work. Data, I think, is at the heart of that chain. But I think you can use the automation, processing power and AI to actually improve the data. That's a kind of starting point."

But while Jon concludes that AI can enhance data processing, he believes human intelligence remains crucial for understanding and leveraging the data.



VIP PARMAR

Global Head of Data Management, WPP

"The hackathons have really brought out a bunch of organic use cases, some that we didn't even know existed and, I think, that's part of the journey as well. People then start to realise what it can do and then how it can be used to achieve great outcomes."

Vip Parmar, Global Head of Data Management at WPP, has a passion for disruptive technology and innovation. He's been with the organisation which he describes as having a strong focus on technical innovation for over five years and his responsibilities cover five areas; data democratisation, data literacy, building out the organisation's communities, running data innovation projects, and governance and compliance. Having always taken an interest in emerging technology, he feels fortunate to have witnessed the emergence of disruptive technologies throughout his twenty-year career in the data world including the World Wide Web in the early 1990s, smartphones in the mid-2000s and, more recently, AI.

"AI's definitely not a fad, it's something that's here to stay. It's going to evolve and grow, and it's something that's already been embedded into our ways of working and our day-to-day lives."

Vip has already identified a number of ways that AI is improving WPP's operational efficiencies by streamlining access to information, knowledge and insights.

"Whether it's analysts that are building dashboards or writing code and being able to use Copilot type services to help them write that code or to validate that code or to optimise code or front-end dashboards or enable expedient testing. So it's really just amplifying and supercharging what we can do, but also at the same time allowing people to do things that they couldn't do before."

Vip's goal is to enable 'human augmentation', where AI exists to help people do their jobs better but humans are still in the driving seat; instructing the AI, evaluating what does and doesn't work, and providing creative flair. He's very aware that some people might have concerns that their roles will be replaced by AI and machines, and will need to be encouraged to embrace it. The company has recently held several hackathons to promote the use of AI and allow staff to explore its potential, and this has resulted in some unexpected benefits.

"The hackathons have really brought out a bunch of organic use cases, some that we didn't even know existed and, I think, that's part of the journey as well. People then start to realise what it can do and then how it can be used to achieve great outcomes."

Vip advises that to fully realise AI's potential, leaders may need to redesign or create new business processes and he warns that simply automating or adding AI to existing processes without evaluation can add complexity, rather than streamline them.

"Sometimes the way we do things is just predicated by the constraints that we have or the things that we use or the components that exist in that particular process. When AI comes into place, it might mean that part of that process is no longer needed...

And there are new things that we probably need to do, like having a human in the loop for checking outcomes, checking handoffs and outputs. There are things that we need to do that we weren't necessarily doing before that we need to adapt to."

Vip believes that AI can give leaders a deeper understanding of their business and assist organisations in their journey to what he refers to as "consciously competent". However, he estimates that currently, only 15% of organisations have access to the data they need to make decisions and service clients so improving data visibility, accessibility and availability is a key priority. Technologies such as AI are enabling this to happen. Indeed, Vip would like to be able to recreate the ChatGPT-like experience over their enterprise data.

"What we've seen with the emergence of OpenAI and ChatGPT is that it's become so easy for anyone to then start to unlock and get those insights ready. You just type away, you ask questions and you can get meaningful answers. You don't have to be able to write code or write SQL or know how to interrogate an API."

Unsurprisingly, as a passionate technophile, Vip would prioritise spending budget on technology before people and process with the primary goal being to unlock value, enable process efficiencies and optimisation. However, he maintains that empowering people is also important so organisations should build tools that provide value and work for people regardless of their skill level or seniority. He also cautions that it's not enough to just buy an expensive tool and expect it to bring immediate gains. Instead, he suggests that people play a vital role in adapting the technology so that it solves specific business challenges.

SARAH HARVIE

Chief Information Security Officer, Kingfisher

" It depends on the environment you're dealing with. Some organisations might be strong in technology but weaker in process, and there's always a people element that needs attention."

Sarah has been CISO at the home improvement brand Kingfisher for just over a year. She's worked in security for over 20 years, previously at Amazon Web Services where she built teams to protect cloud environments, and prior to that as Head of Information Security at Merlin Entertainments, protecting theme parks worldwide, "It was a very fun job!".

Sarah explains how context is an important factor when considering the relative impact of people, process or technology on success.

"It depends on the environment you're dealing with. Some organisations might be strong in technology but weaker in process, and there's always a people element that needs attention."

She describes a recent networking event for security professionals she attended, where attendees took part in a realistic scenario protecting an industrial waterworks and back-office site. Participants were handed a card representing different security controls, each with associated costs and values, with the goal to apply controls according to best practices within a given budget. Interestingly, she explains that even though all the groups faced the exact same situation, every team chose different controls based on their perspectives.

This experience, she believes, really highlights the contextual nature of decision making and the fact that outcomes depend heavily on the CISO in place and the situation they face at the time. Even given the same problem and resources, different leaders will prioritise differently. Sarah acknowledges that although the common ambition of CISOs is to become more of a business partner and enabler, it can be difficult to show how security directly helps the business build value. Sarah argues that the key route to achieving this is by focusing the business on risk.

"We can talk about compliance, control frameworks and technology but unless we truly understand the business's critical processes and assets, we can't have meaningful conversations with business leaders. It's about framing discussions around what matters to them, rather than focusing on abstract threats that may not feel real until after an incident happens. By then, it's too late."

Understanding the critical business operations first enables proactive, impactful security conversations. Sarah also observes how technology teams have evolved significantly over the last decade and IT is no longer just about infrastructure and service desks.

"Now, we have digital, data and product teams which are much more embedded within the business. They are enabling business outcomes directly."

Sarah argues that by aligning security with these teams, embedding security into products and protecting data models, security can get much closer to being a true partner to the business. Sarah is optimistic about AI and its potential as an enabler for security functions.

She explains that CISOs are already using AI to automate detection processes which reduces manual workloads and gives time back to security teams. Automation can also help streamline repetitive tasks and enhance threat detection capabilities, allowing teams to focus on higher-value activities.

"It's not just about efficiency. It's about fundamentally changing how we defend against threats in a landscape that's evolving faster than ever."

Conclusion

This fascinating collection of interviews provides a rare insight into life at the coalface of security and resilience in 2025. It's a world where new, rapidly evolving technologies pose a significant cybersecurity challenge on an almost daily basis. However, importantly, these interviews also reveal how these new tools can also help strengthen organisational resilience and enable business growth.

It's clear that the journey towards becoming a resilient and secure organisation is not without its challenges. All of the organisations we spoke to are experiencing pressure to cut costs and drive efficiencies. Many operate in fast-moving and highly competitive environments so the ability to understand how the environment is evolving and to adapt quickly to changing circumstances is a key driver for technology. Emerging technologies like AI and automation are fundamental to their plans for competitive advantage, and aligning people, processes and technology is crucial for achieving their business goals.

The responses to the questions regarding aspirations and goals were perhaps the most surprising given the current emphasis on cost reduction and efficiency improvement. Rather than focusing on cost savings, head count or ROI, leaders expressed more profound aspirations for automation and AI. These aspirations included improving NHS clinical outcomes, advancing research to find a cure for diabetes and reducing global scarcity.

There's no doubt that these leaders have also encountered significant internal challenges along the way. However, crucially, they demonstrated how they were building strong foundations through their people, processes and technology to help overcome these obstacles. While there were differing opinions on which of the three elements was most important, all agreed they were highly interconnected and that leaders should focus on balancing all three elements, whilst also ensuring they are aligned with business objectives.

AI was unsurprisingly a hot topic of conversation in the interviews and many of the discussions touched on the importance of establishing effective AI guardrails or an ethical framework to help ensure that their AI tools, and the application of AI in their organisation reflect their standards, policies and values.

"In the face of relentless change and mounting pressure we put on ourselves and on our teams, the true measure of resilience lies not just in the technologies we adopt, but in the unwavering commitment to strong servant leadership to align our people, processes, and values with our business objectives."

- Dan Jones, Senior Security Advisor, Tanium and formerly Service Owner (Defensive Cyber Operations) at UK Ministry of Defence

People

Despite being perceived as a more technical function, one of the most powerful themes to emerge from the interviews was the importance of people and the need to manage change effectively to mitigate risks and maximise the potential of new technologies.

There was wide acknowledgement that cybersecurity leaders and their teams face intense pressure, owning responsibility for cybersecurity or compliance failures often without the people and skills to mount an effective defence. There was also agreement that the skills gap is acute, and hiring externally to plug these holes is challenging and costly. Upskilling and training existing employees is a priority for many to ensure that everyone has the skills to leverage new tools effectively and safely. Given that the human aspect is often the greatest attack vector, several leaders also spoke of the need to promote a cyber-safety culture throughout the wider enterprise.

"Skilled staff will assess existing processes, identify suitable solutions and implement them effectively. The NHS has a history of digitising paper-based processes without optimising them for technology which limits efficiency gains. Investing in people ensures that technology is deployed in a way that maximises its benefits."

- Jason Bradley, Chief Digital & Data Officer, NHS Digital

On an optimistic note, the interviews reveal that the response to automation from people has been positive overall. However, leaders also cautioned the need to strike the right balance; using AI for efficiency whilst ensuring human expertise remains at the centre of decision making. Phrases such as 'human augmentation', 'optimise', 'empowerment' or 'supercharging' were used frequently when discussing the potential impact of AI and automation tools on their staff. Everyone was able to give examples of how new tools were freeing people up from mundane or monotonous tasks, and many leaders believed their people were now able to add more strategic value or to "take the driving seat" though better access to data and insight.

"Security professionals enjoy their jobs when they're solving interesting problems, not sifting through endless alerts. Our goal is to use AI and automation to enhance their efficiency, while keeping their roles engaging. AI can help contextualise alerts, filter out false positives and provide actionable intelligence. This allows our analysts to focus on investigations that require human intuition and lateral thinking."

- Duncan Hayes, Head of Cyber Defence, Hargreaves Lansdown

As expected, the issue of people and change management was a recurrent discussion topic with leaders acknowledging the impact of resistance to change or the 'we've always done it this way' mentality that can hamper innovation.

Trust was another concern raised, particularly in the context of AI, and there was agreement that leaders must ensure that teams are involved in the implementation of new technologies and that any concerns they have about the impact of new tools, such as AI, on their roles are heard and addressed.

"Change can feel threatening. Employees take pride in their processes, and challenging those can feel like challenging their expertise. Breaking these habits requires strong sponsorship from leadership and clear communication."

- Julie McCombie, Head of IT, Diabetes UK

Process

The rapidly changing business environment and market demands have made it essential for businesses to modernise their processes. Many interviews highlighted the detrimental impact of outdated legacy processes on business agility, and several referred to the presence of 'friction' between departments and within their processes.

"Flexibility is key. I believe the vision should be about creating security strategies and teams that are adaptable enough to deal with that kind of disruption, react to it and grow that muscle memory."

- Martin Jimmick, Head of Information Security, Whitbread

Several of the companies we interviewed faced challenges because they had scaled so rapidly. They discussed battling complexity and inefficiency due to outdated internal systems not designed for an enterprise setting. Others struggled to scale AI projects beyond the experimental stage due to silos. Leaders emphasised the importance of streamlining and automating workflows, eliminating outdated processes and improving collaboration across departments.

"Traditional processes often require a lot of manual effort and human intervention to move tasks forward. Even with modern service desk software and ticketing platforms providing better control and visibility, we still experience friction."

- Martin Jimmick, Head of Information Security, Whitbread

Leaders agreed that AI and automation would help them to align operational speed with business goals, significantly reducing friction and speeding up initiatives.

"Oftentimes, processes get a bad rep because they are an afterthought or bogged down by organisational debt. Invest time up-front to be clear on outcomes and instrument your process with success metrics so you'll know if you've got it right."

- Hosanna Ouellette, Director of Global Program Management, Spotify

Technology

Perhaps because the interviews were conducted with a group of technologists, there was a general consensus that technology was the 'easiest bit' to get right.

"The technology is generally pretty simple. I say that you can buy a new server rack or you can migrate to cloud, and there are some great cloud providers available and they're secured to the appropriate levels. That's all achievable. The people and the processes are the bit where it gets really interesting to my mind, particularly when you start to scale."

- Jim Green, Technical Director, AI & Data Team Lead, AtkinsRéalis

A recurrent recommendation was that technology choices should be aligned with business goals, and the focus should be on solving business problems rather than implementing technology for its own sake. Leaders also cautioned the importance of always considering the problem it is you are trying to solve rather than the tool itself.

"Don't implement a new technology just because it's there. You want to be looking at what problem or what process you were trying to either improve or get around that a technology or a new tool will achieve. So, no matter which way round, you're not implementing technology for the sake of it."

- Matthew Harriet Randall, Head of Software Development, Automotive company

Hosanna from Spotify agreed and stated that the most important consideration when driving change should be to always lead with business challenges or goals first to avoid being "a hammer looking for a nail". As mentioned earlier, the subject of AI was a repeated feature of the discussions. Indeed, many of the organisations we spoke to are already deploying AI and automation tools to improve threat and anomaly intelligence, and to automate response systems to bolster cyber defences.

One interviewee explained that he believed the AI hype cycle had peaked in 2024, and the focus has shifted from flashy features to practical uses and real-world results. It was clear from all of the interviews that AI is here to stay and has evolved beyond pilot projects and experimentation to implementation. Leaders agreed that it's at this stage that organisations will face challenges with integration, scalability and trust if organisations have not put the right foundations in place.

Jim Green, Technical Director, AI & Data Team Lead, AtkinsRéalis, recommended asking the questions;

"Is new always better?" when the pain of migrating from one software package to another at enterprise level can be so significant? Is the benefit worth it or are you just adding complexity?"

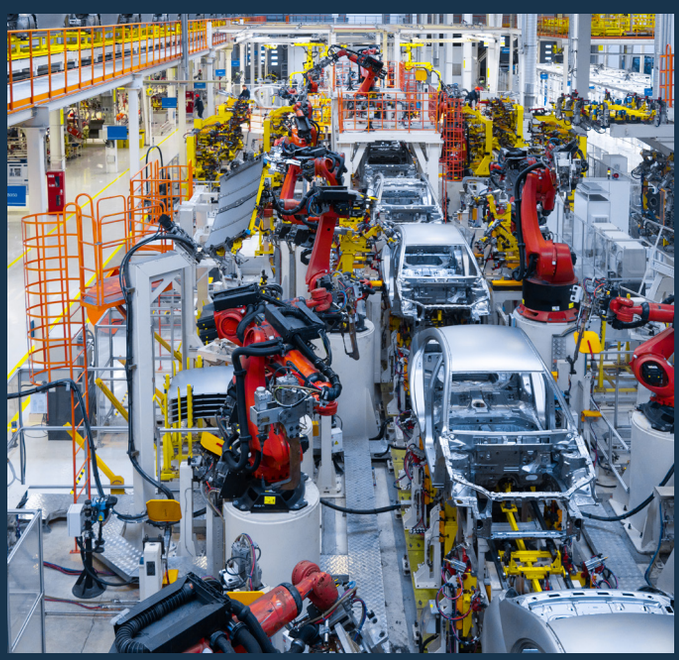
Adopting a Measured Strategy to People, Process and Technology

It's clear from these interviews that people, processes and technology are all essential components of an effective cybersecurity and resilience strategy. This research also suggests that a balanced investment across all three areas will have the greatest business impact in the face of rapid change and escalating threats. While AI and automation tools offer significant potential, human expertise remains central to decision making.

By prioritising collaboration, adaptability and a business-led approach to technology, leaders can position their organisations for success in an ever-changing digital landscape.

"Smart, well-trained individuals will write processes, analyse lessons learned, procure the right technology, run the technology, improve and tune the technology. The great mistake in our industry is thinking that a tool will be the silver bullet. It's not. It's the combination of all three."

- Stuart Seymour, Group CISO and CSO, Group Security, Virgin Media O2



About Chief Disruptor and Tanium

Chief Disruptor is the community for business and technology leaders. Disruptive leaders believe like us, that disruption is a catalyst for opportunity and our name, Chief Disruptor, proudly embodies and celebrates that mindset. Since 2005, our membership community for business and tech leaders has brought together innovators, changemakers and disruptive thinkers to share expertise, strategies and actionable insights.

Our purpose has always been to cut through the hype and enable our members to leverage these disruptive trends and technologies through our member-led insight reports, content and community activities.

With ongoing geo-political unrest and the grim reality of recession on the horizon, organisations now more than ever, need nimble, purposeful leadership that grasps the opportunities and proactively manages the threats of disruption. It's not going to be easy but we are here to help guide you.

Connect. Learn. Disrupt.
chiefdisruptor.com

Tanium is a cybersecurity and systems management company that provides real-time visibility and control over IT environments. Founded in 2007, it specializes in endpoint security, helping organisations detect and respond to threats efficiently. Tanium's platform is trusted by global major enterprises and government agencies for managing and securing vast complex networks.

Tanium Autonomous Endpoint Management (AEM) offers the most comprehensive solution for intelligently managing endpoints across industries, providing capabilities for asset discovery and inventory, vulnerability management, endpoint management, incident response, risk and compliance, and digital employee experience. The platform supports 34 million endpoints worldwide, including 40% of the Fortune 100, delivering increasingly efficient operations and an improved security posture at scale, with confidence, and in real-time. For more information, visit www.tanium.com and follow us on LinkedIn and X.

The Interconnection between People, Process and Technology is a must read for today's and tomorrow's IT and security leaders.

In a world where business transformation is a necessity, cyberthreats are unrelenting and technologies are moving at an ever-increasing pace, IT and security leaders stand at the forefront of these challenges. As organisations race to adopt AI, automation and other emerging technologies, many find the path to value far more complex and pressurised than expected.

The Interconnection between People, Process and Technology dives into this high-stakes landscape, offering candid insights from 23 global IT and security experts. Through in-depth interviews, this research explores how the right balance of people, process and technology can unlock lasting business impact, resilience and innovation. Whether you're navigating prototype pitfalls or striving to scale smarter, this book delivers vital lessons from some of the smartest organisations turning IT complexity and security resilience into competitive advantage.

Bold, insightful and refreshingly honest.