THE FUTURE CIO

02 TECH TALENT
How CIOs can prepare for an IT skills exodus

06 INTERVIEW
UK cyber chief on how business can protect itself from threats

12 SMES
What to know when hiring your first ever CIO

TRENDS

CIOs look to the world after Covid

CIOs stabilised their businesses in the pandemic, but they're now focused on the post-Covid business world. We look at their in-tray for the coming year

Jonathan Weinberg

CIOs have been in the driving seat during Covid-19, not least navigating the challenges of working from home. But as the new year approaches, they're hoping to put the pandemic to one side and focus on new priorities.

There's plenty to keep them busy in 2022, from tackling skills and talent gaps to firming up cybersecurity protections and working more closely with CFOs on budgeting. Conor Whelan, CIO at multinational consumer credit reporting company Experian, thinks operational resilience should be near the top of the agenda. Both regulators and customers are focused on the concept of "never down", according to Whelan.

"It is easy to say, but hard to deliver, especially in any organisation that has a blend of heritage systems and new digital cloud native systems. Easy to do in the latter but harder to do in the former."

Whelan believes operational resilience isn't just about the technology you have in place; it's about having the right people and processes to deal with problems when they occur. Companies must consider how they're stress-testing their own on-premise or cloud solutions, while ensuring that the organisations supporting their own product development and maintenance activities are doing the same. This should include asking how these businesses are testing their end-to-end supply chain, he says, to be ready if something goes wrong.

"As you migrate more to the cloud, are you really looking at your third-party components that you are using in that cloud ecosystem? What operational resilience and capabilities have those companies deployed?"

You're only as strong as your weakest link, Whelan warns.

"That's so true in technology. I see more pressure from customers who are actually prioritising operational resilience over new features and new functions, and I think that trend will continue through 2022."

Another growing focus for CIOs hits very close to home: the nature of the job itself. They must find the right balance between their roles as tech leaders and as business leaders.

"CIOs' profiles have been elevated in the last 12 to 24 months," says Whelan. Even smaller, tactical activities like overseeing remote working have given them a good seat at the table. They must now look to the future of their new, elevated positions.

"For me, it's about deepening your understanding of the business you work in, getting that deep business process knowledge and expertise."

Going forward, the job is to ask how CIOs add more value, he notes.

"You're going to have to be better at that balancing act between 'run and maintain' versus 'grow' versus 'transform'," says Whelan. "These are the tough decisions businesses have to take on a regular basis and you need to do your homework to bring data to the table to fight your corner and engage in growing your organisation."

> **We've all depended on digital during the pandemic, so it's essential to make system interfaces intuitive for all users from Gen Z to Boomers**

Of course, many of the challenges CIOs have experienced over the past 12-18 months will still be high on the to-do list in 2022; they include hybrid working, the ongoing implications of Brexit, a rise in AI adoption and moves towards net zero.

But the one that appears to occupy most minds right now is finding talent.

Stephen O'Donnell, CIO at workplace pension provider The People's Pension, says that as "the relentless pursuit of digital continues", demand for high-quality software engineers and testers, cloud engineers and dev-ops specialists is at an all-time high across the world, challenging the norms for CIOs.

"Wages are continuing to rise at unprecedented speed as London pay rates become available for engineers based in the regions who can telecommute," he explains. "Brexit has not helped at all as many highly talented developers have gone home, shrinking the available UK workforce."

O'Donnell describes the expansion of HMRC's IR35 regime - designed to assign many full-time contractors as employees - as "the straw that is breaking the camel's back", as it dramatically reduces the availability of the flexible workforce that CIOs need.

"Winning and retaining talent is the current battleground that CIOs are engaged in."

The experiences of current workforces, however, are also key to 2022's challenges. Covid-19 has changed the nature of the office, with employees accustomed to working on their own technology deployed in their own environments.

Heather Bunyard, CIO at global media insight company Cision, believes CIOs face an ongoing mobile device management challenge. She says a comment from her own son gave her a glimpse into what next year could hold; he preferred to play online games on his own PC at home, rather than sharing a single device at his friends' houses.

"His response was: 'It is no fun because we cannot play when we are together'. He then explained he needs to be on his own PC. I am seeing this same blend of the virtual and physical world at work."

Bunyard cites the example of a colleague who recently requested to take a meeting from his own desk, rather than in a conference room, as he felt it would be easier to collaborate from his own computer. She says Covid-19 has changed many things, forcing us all to maximise our efficiency. "We have learned new online strategies and techniques, which will require us to adapt and evolve how we work together in a highly blended work environment," she adds.

Helena Nimmo, CIO at software development company Endava, believes data, automation and user experience are key for 2022, internally and externally. Data-driven information must reach those who need it, when they need it, and in whatever form they need.

"User experience has never been more critical," she says. "We've all depended on digital during the pandemic, so it's essential to make system interfaces intuitive for all users from Gen Z to Boomers."

But as we look ahead to 2022, Nimmo sees a danger on the horizon. As technology infiltrates every area of business, CIOs have become responsible for the wider landscape, everything from operations to innovation and – most importantly – the customer experience.

"The weight of these often-competing pressures and responsibilities can be intense, and ultimately a major contributing factor to the fact that the CIOs, on average, have the shortest tenure of the whole C-suite," she warns. "Ensuring there's a strong network of systems and people in place to help CIOs grow into the leaders they've become, while being able to delegate outward, will be crucial in the coming year."

TOP TECH TRENDS FOR 2022

Gartner, 2021

Technology research and consulting company, Gartner, highlights the following 12 technologies as the innovations driving organisations forward in 2022

1	Data fabric	Integrates data across platforms and users, making data available everywhere it's needed
2	Cybersecurity mesh	Provides a composable approach to security (rather than a fragmented one), based on identity, to create a scalable and interoperable service
3	Privacy-enhancing computation	Allows data to be shared across ecosystems. Approaches include encrypting, splitting or preprocessing sensitive data
4	Cloud-native platforms	Use the core elasticity and scalability of cloud computing to deliver faster time to value
5	Composable applications	Made up of packaged-business capabilities (PBCs) or software-defined business objects, they can save fusion teams time and effort
6	Decision intelligence	Improves organisational decision-making by modeling decisions through a framework
7	Hyperautomation	Identifies, vets and automates as many business and IT processes as possible using tools such as RPA and low-code platforms
8	AI engineering	Discipline of operationalising updates to AI models, using integrated data and model and development pipelines
9	Distributed enterprise	Virtual-first, remote-first architectural approach to digitise consumer touchpoints
10	Total experience	Interconnects customer experience, user experience, employee experience and multiexperience to create a better experience for all
11	Autonomic systems	Self-managing physical or software systems that learn from their environments and can modify their own algorithms without updates
12	Generative AI	Form of AI that learns a digital representation of artifacts from sample data and uses it to generate new, original, realistic artifacts

Distributed in THE SUNDAY TIMES

Contributors

Cath Everett
Journalist who specialises in workplace, people and leadership issues, which includes what it means to be an ethical business.

Mark Frary
Award-winning journalist and author of 12 books who writes on business, technology and science.

Emily Hill
Journalist and author, she is the former commissioning editor at *The Spectator* and feature writer for *The Mail on Sunday*.

Christine Horton
Long-term contributor to specialist IT titles, she writes about technology's impact on business.

Andy Jones
Journalist and broadcaster who has written for every major national newspaper and produced business packages for BBC World Service and TV for BBC1/2 &C4.

Charles Orton-Jones
PPA Business Journalist of the Year, former editor of *EuroBusiness*, specialising in fintech and high-growth startups.

Oliver Pickup
Multi-award-winning journalist specialising in business, technology, sport and culture.

Jonathan Weinberg
Journalist, writer and media consultant/trainer specialising in technology, business, social impact and the future of work and society.

Sally Whittle
Experienced business and technology writer for national newspapers and B2B magazines in the UK and US.

raconteur reports

Publishing manager
Olly Eyre

Managing editor
Sarah Vizard

Deputy editor
Francesca Cassidy

Reports editor
Ian Deering

Sub-editor
Neil Cole

Head of production
Justyna O'Connell

Design and production assistant
Louis Nassé

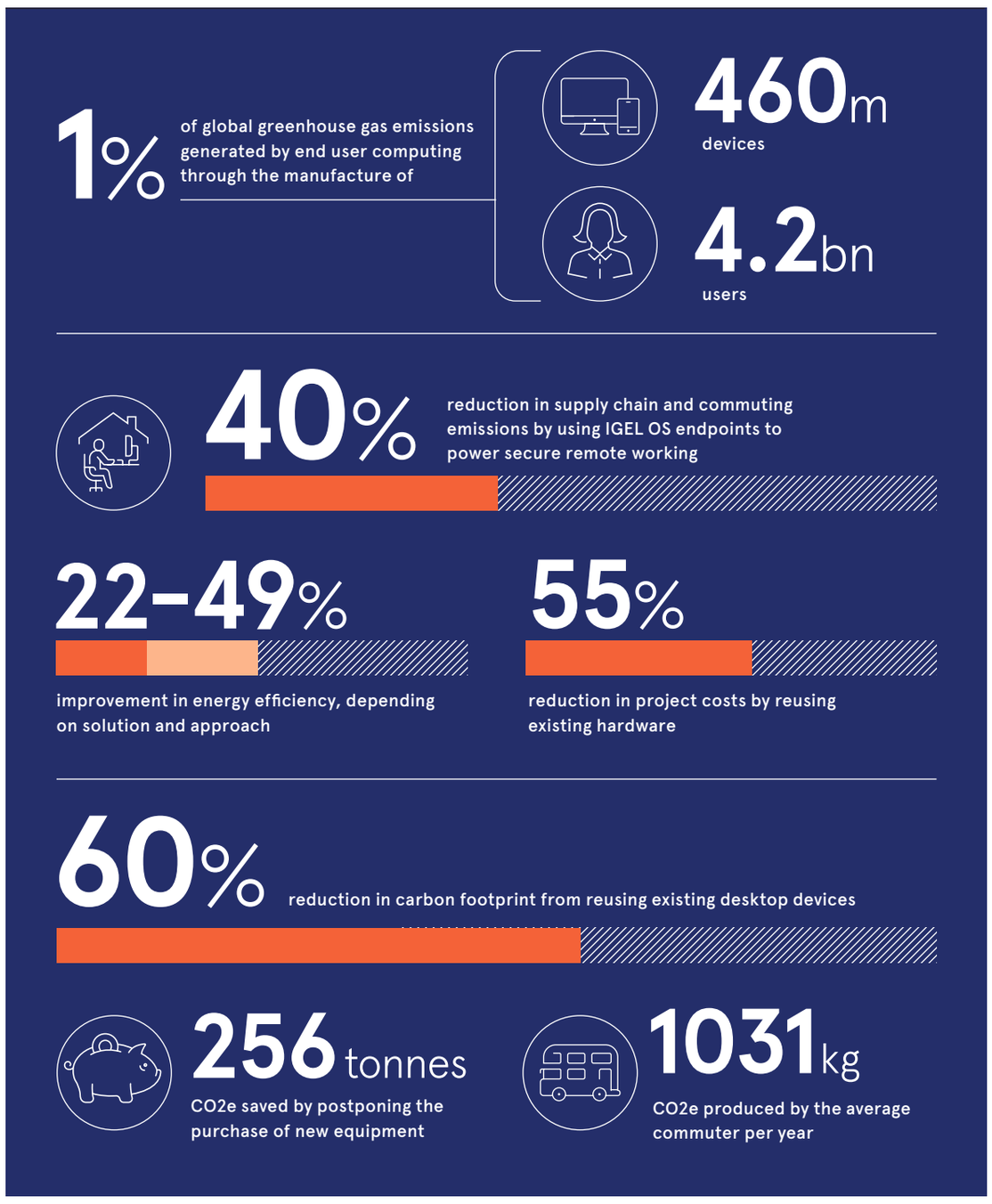
Design
Pip Burrows
Kellie Jerrard
Colm McDermott
Samuele Motta
Nita Saroglou
Jack Woolrich
Sean Wyatt-Livesley

Illustration
Sara Gelfgren
Celina Lucey

Art director
Joanna Bird

Design director
Tim Whitlock

Commercial feature



Think differently to beat disruption, boost security and achieve sustainability goals

The decision to stop constantly upgrading your hardware could hold the key to future-proofing your business

There's an old curse that says "may you live in interesting times". The essence being that 'interesting' means chaotic and uncertain rather than constant and stable. If there is one thing that could be said about current times, it's that they're certainly interesting.

Supply chains are in disarray, commerce is operating on a 'where we are this week' basis, individuals are getting used to new ways of working while they and their employers are coming to terms with the likelihood that we will never go back to the way things were. Both in the short and long terms, we are learning that we must all adapt if we are to thrive and survive.

So in today's 'interesting times', we face three important challenges. The first is remote working. The future of work for many organisations will be their ability to securely access their business applications and data from anywhere. Having rushed to equip staff so they could stay productive at home, the unintended consequence was to open companies up to much greater risk of cyber attack. Instead of 10,000 devices housed in perhaps two offices, they're now spread across 10,000 households.

With staff blurring the lines between personal and professional computer use, emails opened on work on computers, lax use of the company VPN and activities that would otherwise be avoided in an office environment, they are now at far greater risk of ransomware, for example. Companies are keen to avoid rolling out the red carpet, while enabling remote working.

The second big challenge goes back to those supply chain challenges and the worldwide chip shortage. A dramatic increase in demand for at-home computers and mobile phones – even inkjet printers – has arrived at a time when supply chains of all the necessary parts, but particularly the chips, are breaking down. Companies are also in competition with car manufacturers, heating companies, entertainment systems and even the computer companies themselves, whose own drive for innovation means changing up otherwise perfectly well functioning hardware to meet the new upgraded capabilities.

And the final challenge is the rising interest in sustainability. Formerly around position eight or nine on companies' lists of priorities, today it has risen to third or perhaps even second place. In trying to reduce their carbon footprint and achieve net zero, hybrid working has become an enticing solution. Less commuting, smaller office footprint, fewer pieces of hardware and more software and data hosted in the cloud all make meaningful, positive contributions to sustainability.

For many, finding solutions will mean challenging a lot of perceived wisdom. Put simply, we can't keep doing things the way we were.

For the last 25 years, computer manufacturers and the businesses buying their technology have been stuck on an upgrade-driven system. Organisations have been deploying their data and applications via PC and laptops that, for the most part, run Microsoft Windows. Intel has been in a process of constant improvement updating its chips and Microsoft then updating its software to match.

It happened again most recently with Microsoft upgrading to Windows 11, meaning more security, more chipsets and more, newer laptops. Add in the need for people to work effectively from home and there is a perfect storm of large organisations like the Department for Work and Pensions (DWP) buying in tens of thousands of devices.

> **Companies need to wean themselves off their dependency on a traditional, locally installed Microsoft operating system and consume Windows from the cloud**

It doesn't have to be this way. The life of an existing PC can be extended for at least two years. Even a small, 3000-seat organisation can save 40% of their carbon footprint. To do that, companies need to wean themselves off their dependency on a traditional, locally installed Microsoft operating system and consume Windows from the cloud – that is desktop as a service, or DaaS.

Accessing virtual desktops from the data centre or the cloud isn't new. Citrix, VMware, AWS and Microsoft all have offerings in this space which allows employees to access their Windows Desktop which looks and behaves, to all intents and purposes, as it always has done. But, by having the operating system running in the cloud, not only is data inherently more secure, but users are much less reliant on the recency of their hardware so there is similarly a much less pressing need to upgrade software and laptops to access current functionality and security standards.

This is where IGEL comes in. An ultra-secure, Linux-based operating system, which replaces Windows on the employee endpoint and connects people to the cloud. There are approximately 100 million cloud-delivered desktops in operation today and IGEL's CEO, Jed Ayers, predicts that number will grow by 50% in the next three years. Gartner is forecasting that 30% of VDI (virtual desktop infrastructure) desktops in 2023 will be DaaS.

All the while, there are currently an estimated one billion standard Windows desktops running on increasingly obsolete hardware and unsupported OSs, leading to a frustrating user experience and worryingly lax cybersecurity. But with an OS like IGEL, coupled with a cloud-delivered desktop, those endpoints, already beginning to age at three years old, can be effective for a further three to five years, allowing employees to work securely from home as well as move the company closer to its carbon neutral goals. All while getting round the chip shortage conundrum.

With the last pandemic scarcely in the rear-view mirror, the reality is that the world already needs to prepare itself for the next one. We need to appreciate the fact that at least 50% of businesses believe the future of work has changed permanently. So the way we traditionally deployed IT solutions and end user computers must also change. Every organisation is on a journey to the cloud with more and more apps being delivered via a web browser rather than desktop OS. So ask yourself, "do companies really need that expensive, hard-to-secure PC on a desk?"

More than a quarter of a century ago, the pinnacle of technological innovation was a Rubik's Cube, the Sony Walkman and a Windows PC. Today, we have Candy Crush, Spotify and... a Windows PC. Why? With a move to the DaaS and VDI, the way the world wants – needs – to work in the future can finally accelerate at the pace of other innovations, protecting the planet into the bargain.

For more information please visit igel.com

MoMo Productions via GettyImages

SKILLS SHORTAGE

Talent competition: the battle for tech skills

As economies reopen around the world, the tech skills crisis is hitting epic proportions. How can CIOs compete for employees?

Cath Everett

CIOs have long grappled with a shortage of crucial tech skills. But as economies recover around the world, the recruitment challenge is reaching new heights.

The pandemic resulted in a lot of projects being put on hold, notes John Nash, founder and chairman of tech recruitment agency Nicholson. But as budgets are released again, it's creating a raft of new jobs and vacancies.

That's not the only challenge. Lockdowns unleashed a wave of digital transformation that continues today, further boosting demand for talent.

And in the UK, the exodus of tech skills since the Brexit referendum has been a key issue, one that has "had a major impact", says Nash.

To make matters worse, as many as 82% of the 2,120 senior technology decision-makers surveyed globally for Harvey Nash Group's 2021 Digital Leadership Report believe the pandemic has, in many instances, changed employee priorities, which include wanting a better work/life balance. Staff retention is more difficult as a result.

The problem is now so severe that just over two thirds of the CIOs questioned are unable to keep up with the change their business requires due to a lack of available talent. Skills in particularly short supply include cybersecurity (43%), demand for which has risen by 23% over the last 12 months alone; big data and data analytics (40%) and technical architects (34%).

So what's the answer to the "Great Resignation", as it's called in the US? Getting into salary bidding wars is rarely the answer, even at a time of rampant wage inflation, warns Nash.

"If you ask people to put their priorities in order, money is nearly always ranked at three or four," he says. "But in tech, you find managers or founders focus too much on that and less on the things that create job satisfaction, which most people put at number one."

Number two on the list is generally career development, Nash adds, while location and job security are often interchangeable with pay.

Failing to truly understand what makes staff tick means employers also fail to tackle the underlying causes of any dissatisfaction – and why employees want to leave.

Sandeep Sakharkar is CIO of global contract logistics company GXO Logistics, managing a team of 1,000 people. He thinks there are four considerations for engaging, motivating and retaining tech workers.

The first is to create an authentic culture in which people actually want to work, while also feeling that they're doing something meaningful. Part of this means ensuring everyone – including the CIO – lives and breathes the company's values and purpose so they permeate through all areas of activity. "It's important that values are seen in action," he says.

A key element here is engaging on an emotional level with staff through clear and regular communication at a group and/or personal level. If personal, two-way communication isn't possible with everyone, it's vital to create an effective management tier below the CIO.

The second factor relates to staff recognition and reward, which must be linked to tangible outcomes. This means not only giving praise where praise is due, but also responding to good ideas and ensuring employees feel empowered to express them.

Next, provide a structured learning and development programme that caters effectively to the needs of both the individual and the business. This is linked to the fourth and final piece of the puzzle: ensuring effective, tailored career development and a clear career path.

"Attrition is a reality for everyone and it's impossible not to have it," Sakharkar says. "So to succeed today, you really need to have a structured, intentional focus on all of these four areas, and also track your programmes to see how they're performing against objectives."

Mark Murphy is director of HR at BT's Technology business, which employs about 11,000 people. He thinks that in the technical community, there's a close link between staff retention and offering interesting and challenging work.

While you've got to be credible on compensation and other basic requirements, "the intrinsic nature of the work, the opportunity to create something new, and the culture and purpose of the business are the elements that make employees want to stay," he says. "People tell us that it's keeping them stretched that keeps them here, which includes the opportunity to learn new skills and work in different parts of the business."

But Murphy believes CIOs themselves also have a major role to play in retention terms.

"An inspirational tech leader is super-important both internally and externally," he says. "Externally, building pride in what the team is doing helps build momentum and recognition of achievements, but internally it's about inspiring people and setting the tone for what meaningful work is."

Nash agrees. "The old adage that 'people don't leave companies, they leave managers' is as true today as it ever was, especially in tech, as all too often people with strong technical skills are put in charge of people without necessarily being the best people managers," he says.

As a result, Nash believes the secret to retention is understanding why employees might want to leave and creating an atmosphere in which they want to stay.

"It's about getting the management team right because if people feel valued, listened to and recognised for what they do, if they have a good work/life balance and a clear career path, they won't leave as they'll know they're working for a great employer."

23%

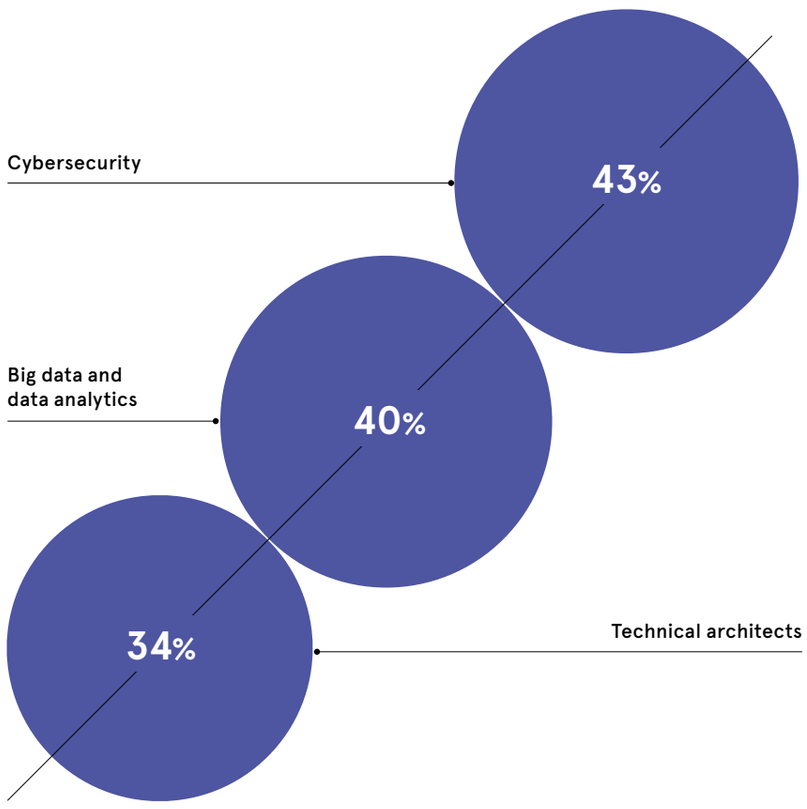
increase in demand for cybersecurity skills in the last 12 months alone

Harvey Nash, 2021

> **The intrinsic nature of the work, the opportunity to create something new, and the culture and purpose of the business are the elements that make employees want to stay**

MOST IN-DEMAND SKILLS FOR CIOS' TEAMS

Percentage of global senior technology decision-makers who say the following skills are in particularly short supply



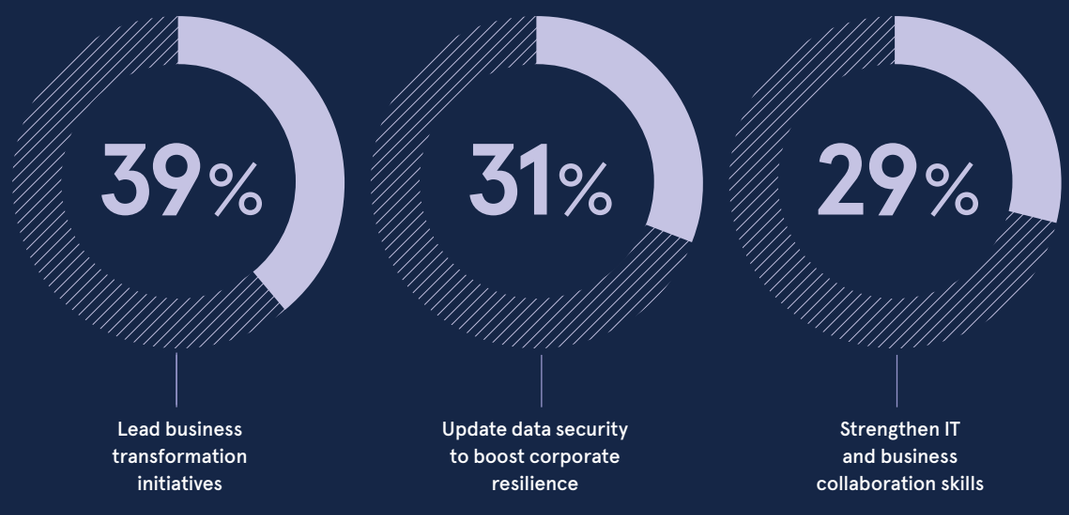
Harvey Nash, 2021

CIO FOCUS FOR 2022

If the chief information officer (CIO) role was already shifting from tech expert to strategic business leader, the pandemic certainly served to accelerate this move. But, now that the CIO's remit has expanded, they must choose their priorities carefully. From allocating budget to the right new technologies, to shoring up security, to addressing the skills shortage, where are CIOs focusing their energies going forward?

WHAT BUSINESS LEADERS EXPECT FROM THE CIO

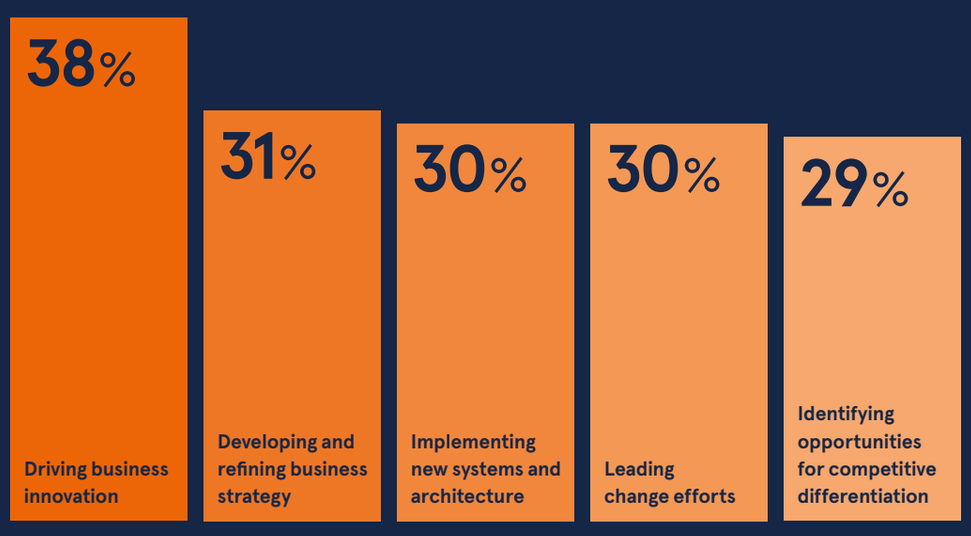
Percentage of IT leaders who said their CEO expected them to do the following things



EY, 2021

WHAT ARE THE CIO'S FUTURE PRIORITIES?

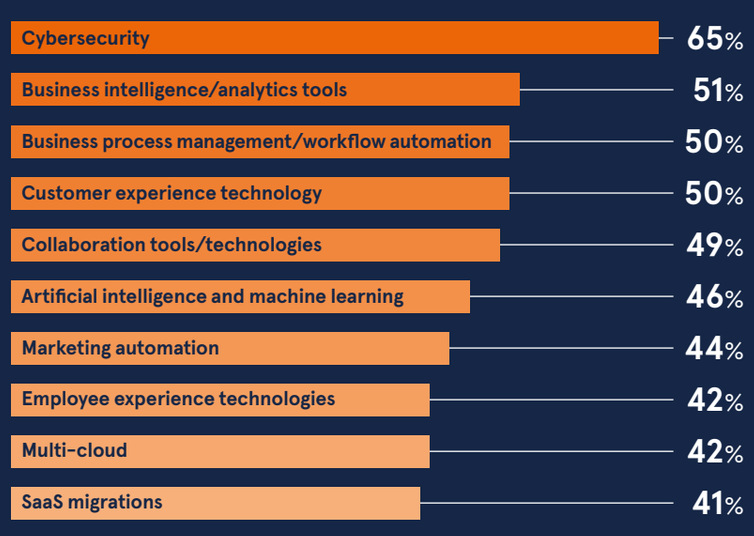
Percentage of global IT leaders who say they hope to focus on the following activities over the next three years



IDG, 2021

WHERE ARE CIOS SPENDING THEIR BUDGET?

Percentage of global IT leaders who say they are increasing spend in the following areas



IDG, 2021

63%

of CIOs say business and leadership skills are more important than technology skills

EY, 2021

80%

are educating CEOs and other senior stakeholders on the value of IT

EY, 2021

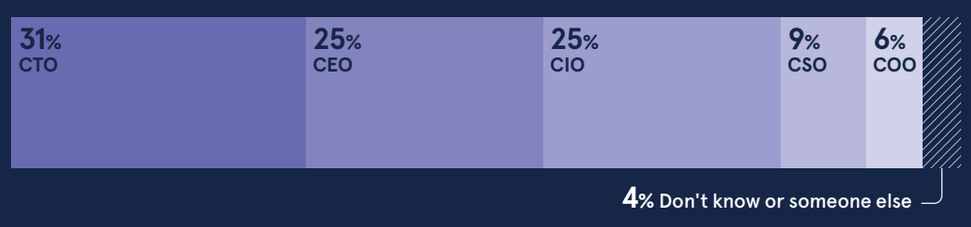
CYBERSECURITY AT THE TOP OF THE CIO AGENDA

Percentage of CIOs who said the following were their top three concerns as a result of Covid-19

PwC, 2021

WHO'S HELD RESPONSIBLE FOR SUCCESSFUL CYBER ATTACKS?

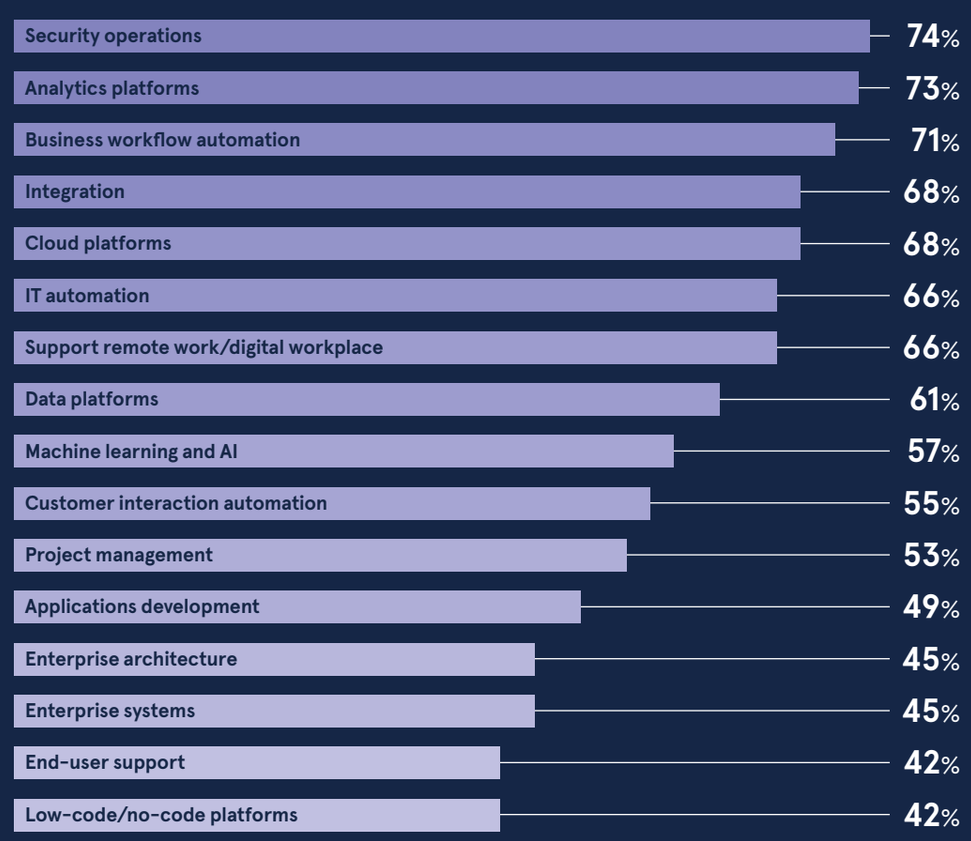
Percentage of senior IT decision-makers who say the following roles are held responsible internally if a cyber attack is successful



Keeper Security, 2021

HOW CIOS ARE CHANGING THEIR TEAM'S PRIORITIES

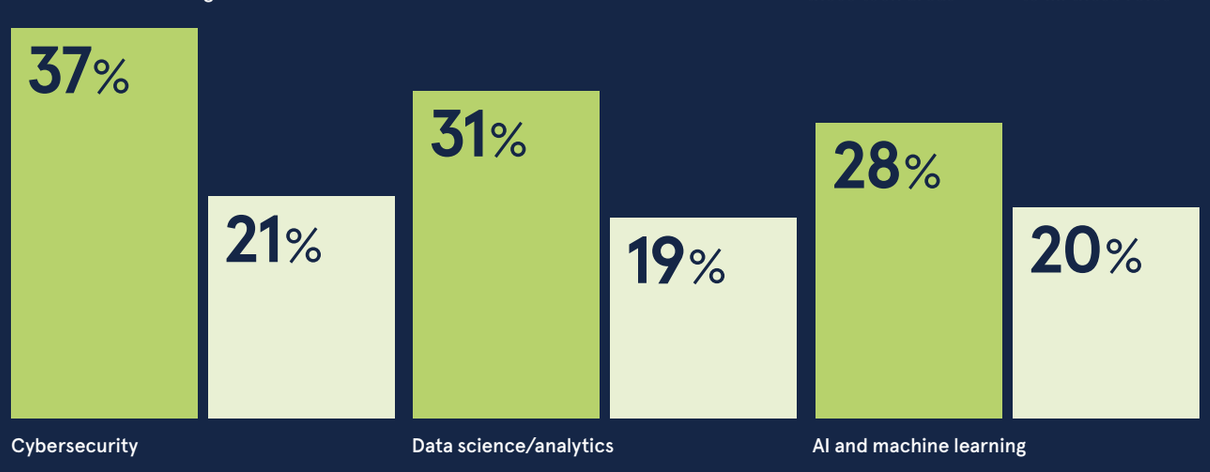
Percentage of global CIOs who say they are likely to expand the following IT activities for full-time employees by at least 2%



IDG, 2021

TOP SKILLS THAT CIOS ARE LOOKING FOR

Percentage of IT leaders who say they are looking to hire in the following areas



IDG, 2021

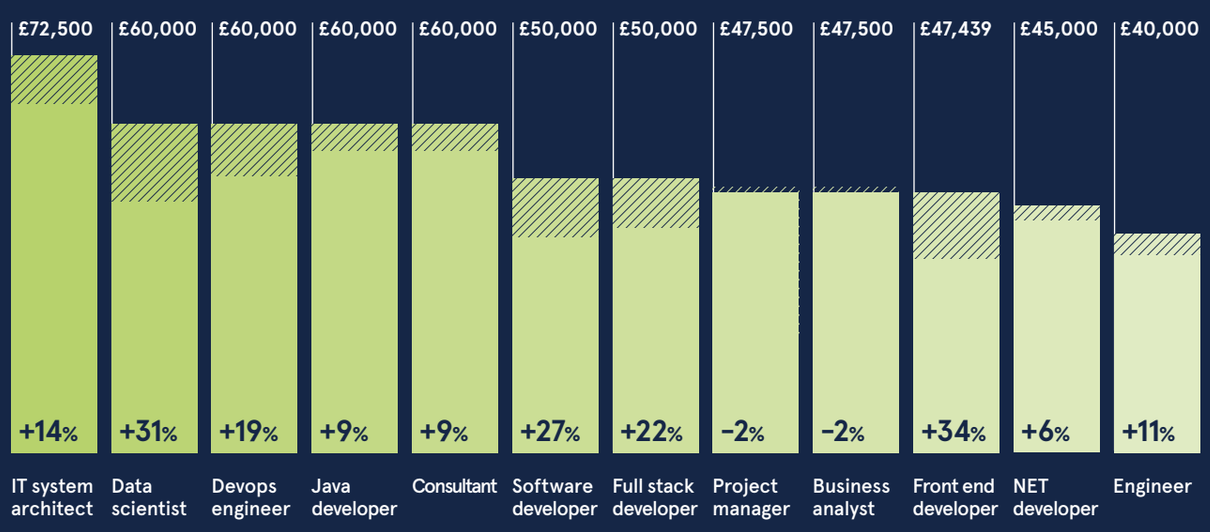
IS THE SEARCH FOR TECH SKILLS GETTING EASIER?

The number of tech jobs advertised in the UK in June of the last three years

Tech Nation and Adzuna, 2021

WHAT ARE THE MOST IN-DEMAND ROLES WHICH CIOS ARE LOOKING TO FILL?

The tech roles which command the highest salaries, according to an analysis of over 17 million rows of job advertisement data



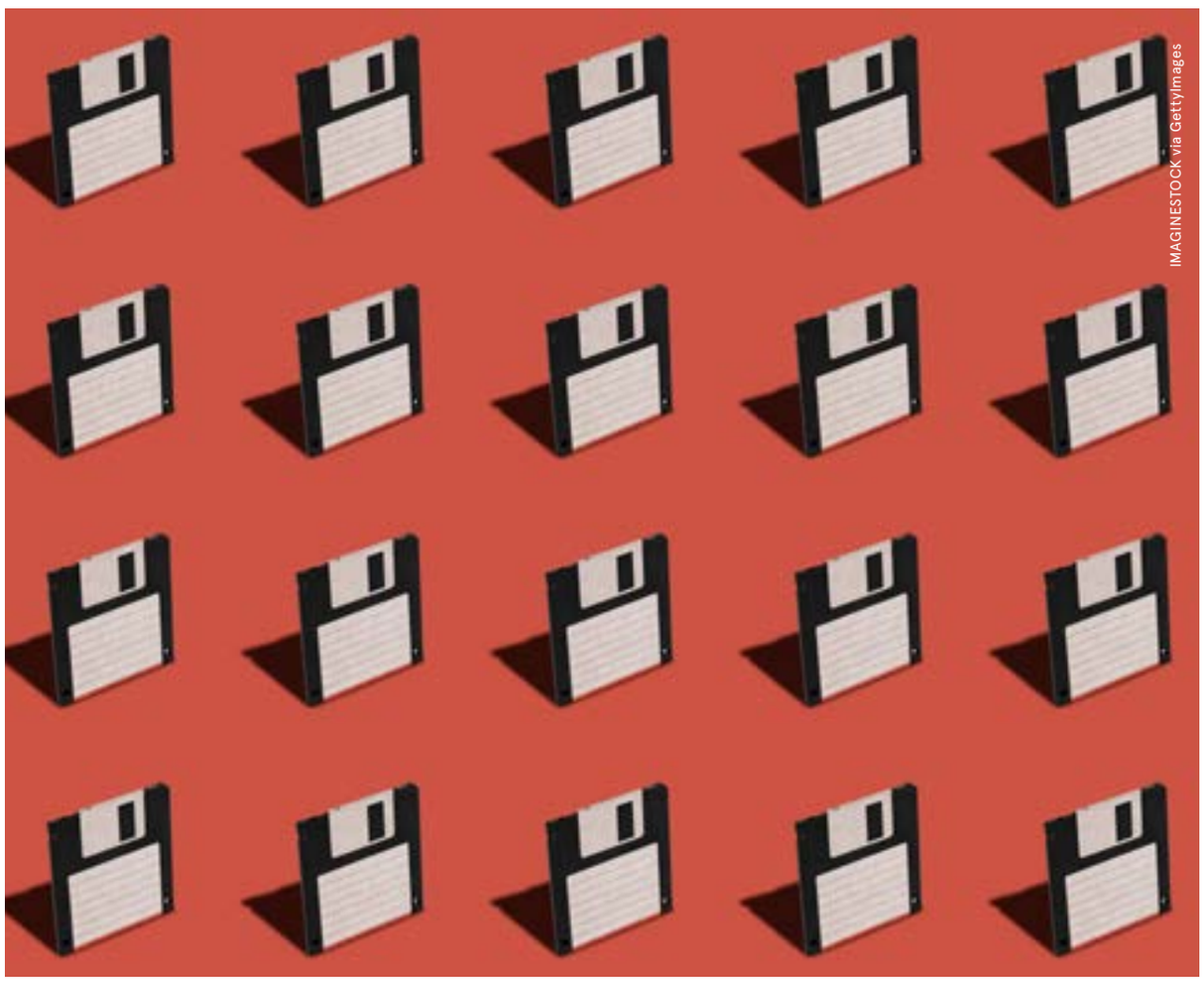
Tech Nation and Adzuna, 2021

DISASTER RECOVERY

Ransomware: a CIO's recovery guide

The pandemic has seen a surge in ransomware attacks. What should firms and their CIOs do if their systems are infected?

Mark Frary


IMAGINESTOCK via GettyImages

There have been many business winners in the pandemic, from online retailers to PPE suppliers to Zoom. Unfortunately, ransomware hackers are part of this lucky group.

Ransomware attacks have increased by 102% in 2021 compared to 2020, according to Graeme McGowan, a fellow of the Chartered Institute of Information Security and cyber risk and security consultant for ESA Risk. He says this is, in part, due to the rise in working from home, which meant many employees were using their own devices on poorly secured home networks, often without proper IT support.

The danger, then, is very real. However, Conor Byrne, managing director of Cribb Cyber Security, notes that "companies have often made some efforts to block the ransomware attacks but often don't have a plan in place for how to deal with an attack."

So what should companies and their CIOs do when they suffer a ransomware attack?

The temptation for many companies, particularly those that have no disaster recovery plan in place, is to pay the ransom. The question is, should you?

McGowan's answer is an emphatic "no".

He says: "There is no guarantee that the perpetrator will free up your network and its data. Not only will you be paying a criminal group, but you are also more likely to be targeted in the future."

Some cybercriminals do send the decryption key, but others simply take the money and run, knowing there are many more targets out there. A survey from cybersecurity specialist Sophos found that 92% of targeted companies didn't get all their data back.

"Attackers often won't release the encryption keys, but they will take and sell your data," says Byrne. "This may lead to the ICO delivering large fines for the information breach."

When a ransomware attack occurs, time is critical. Call on in-house expertise if available or seek help from a third-party cybersecurity expert.

The first step is to contain the breach by isolating infected device(s) from other computers and storage devices. Disconnect them from the internet, whether through wired, wireless or mobile connections. Any networked computer can be a spreader.

Once contained, the nature of the breach should be investigated. If you've received a ransom note, you may know which ransomware has infected your system – this can help with disinfection and removal.

You'll likely need to conduct a deeper forensic investigation. This includes identifying which accounts were accessed and where the attacks came from. It means analysing system logs in detail.

As soon as you know what you are dealing with, you can start to eradicate it. This includes resetting passwords, removing malware, and closing ports. The Europol-backed No More Ransom project includes tools to deal with commonly used ransomware, such as Prometheus and Ragnarok.

Only when you have removed all traces of the ransomware can you restore the network. This isn't simply a matter of reconnecting computers to the network. Administrators will need to reset login credentials, especially administrator-level accounts, wipe infected devices and reinstall the operating system. It can be a lengthy process.

If you've invested in regular backups, you can now restore the system to health. However, you must first verify that any backup you use is free from malware. Using a system restore – effectively turning the system clock back to a time before the infection – is usually not sufficient.

It's easy to focus only on the technical aspects but communicating with stakeholders is vital. This includes your bank, the police and your insurers, as well as employees, clients and suppliers.

Companies are often reluctant to reveal the breach, fearing bad press or a plummeting share price. Yet if news leaks, trust can be lost. Develop a communication strategy so that the right information reaches the right stakeholders in a timely fashion. This will help ensure you comply with any breach notification laws.

It's important to understand how critical the issue is and its effect on operations before notifying external parties. The worst scenario is that a panic ensues, with teams unable to focus on recovering the systems and operations.

Once you've restored your networks, monitor them for at least two weeks to ensure they're "clean". The UK's National Cyber Security Centre, in conjunction with four other international cybersecurity agencies, has a much more detailed technical advisory for companies who have fallen victim to ransomware.

If you survive the attack – and a large proportion of companies do not – putting a disaster recovery plan in place that ensures data is backed up is vital. This means that in the event that your data is encrypted and held ransom, "you are not subject to paying a ransom and hoping for the best," says McGowan.

"By investing in disaster recovery, you are investing in control. Only businesses that invest in a hardened security posture, as well as a validated disaster recovery programme that tests and restores data backups from off-site and preferably offline locations are adequately prepared."

Byrne says: "If you are only going to do one thing, carry out a restore from backup. So many companies think their backups are good and then they fail on restore. Do a recovery at least once per year."

Companies also need to invest in helping employees identify threats, he says.

"As ransomware is basically a con trick, it is really important that the users recognise the emails and communications that lead to an attacker being able to get the ransomware onto their computer."

> **Attackers often won't release the encryption keys, but they will take and sell your data**

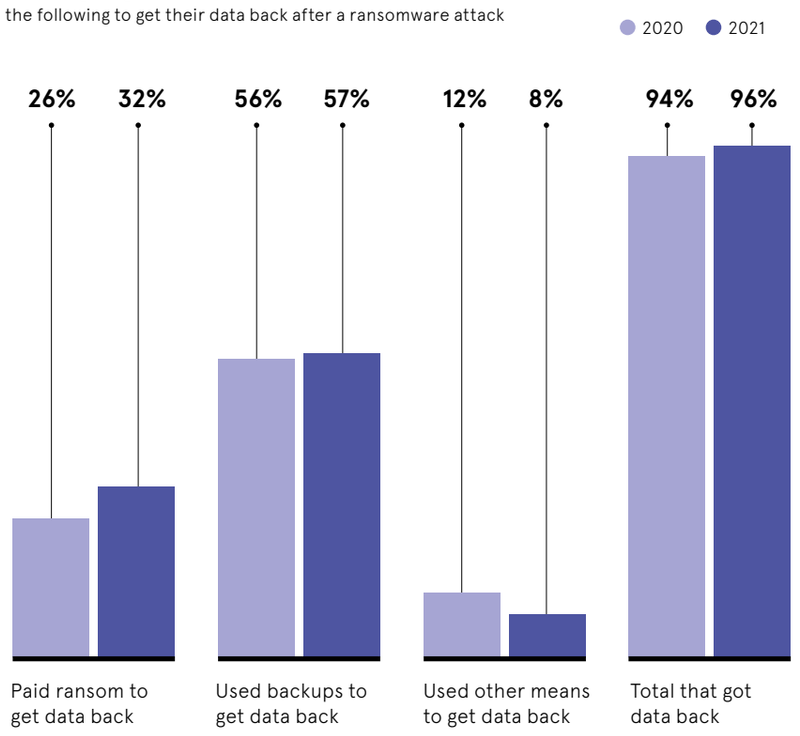
All companies should also implement a trusted cybersecurity and information governance framework such as the UK's Cyber Essentials Plus or ISO 27001. Then employ an external security advisor and external data protection officer who can audit what's been done to ensure it is fit for purpose.

And, according to McGowan, the problem isn't going away.

"As a CIO, how am I going to manage the new world of work? I may have 50 members of staff but only three permanently in the office with the rest scattered around the UK. It is going to be a prevalent issue for a long time to come."

RISE IN RANSOM PAYMENTS

Percentage of global IT decision-makers who said they did the following to get their data back after a ransomware attack



Sophos, 2021

COLLABORATION

Numbers game: working with the CFO

To secure IT investments, it's vital that CIOs speak the same language as the CFO and other members of the C-suite


10'000 Hours via GettyImages

Christine Horton

On Nike's latest earnings call, CFO Matthew Friend made the business case for IT investment. By investing in areas like digital fulfilment, predictive modelling and personalisation, digital revenue was about 10 points higher than wholesale revenue.

CFOs use such cold, hard facts when agreeing CIOs' budgets. Friend's comments suggest Nike's CIO had succeeded in selling the importance of IT investment.

Today, CIOs are more than tech specialists; they're strategic members of the C-suite. The modern CIO must be just as comfortable talking to board members as they are to members of their own team.

That's especially true when making the case for investment, where it's essential to speak the CFO's language. A global survey by Deloitte Global and Workday shows that 60% of "progressive" CIOs see strategic partnerships with the CFO and other stakeholders as key to succeeding in the role. These CIOs try to ensure their priorities are strategically aligned with those of the wider business and well understood by all key stakeholders.

"As a CIO you're going across all the different departments, you've got to talk the same language as everyone you're dealing with. The CIO has gone from being someone who's very technical to someone who's about finding solutions and delivering value, and therefore that language has got to change," says Gerard McGovern, CIO for The Guide Dogs for the Blind Association.

It's fundamental that CIOs understand the language and the nature of business, McGovern says. They must be able to demonstrate a clear understanding of the return on any investment and present it in compelling language that the CFO understands.

"So you're talking about net present value, return on investment, discounted cash flows. You're not just saying, 'well it is going to cost £100,000, it is going to give us £100,000.' Because the CFO will turn around and ask: 'Is that £100,000 now? Is that £100,000 In five years' time? What is the return?'"

However, it's important to recognise that not all IT investments are the same. Stephen O'Donnell, CIO at workplace pensions provider The People's Pension, points to three types of IT systems.

First is "commodities", where the critical success factor is to keep them running reliably and as cheaply as possible: email and document management systems, for example. Second is legacy systems "where executives are only interested if the regulator or ICO has them in their sights". Finally, there are key systems that "move the business needle and are core to delivering a competitive advantage for the organisation", like digital customer-facing systems, logistics platforms or other critical applications that "executives are desperate to invest in".

It's this third investment type that's caught the attention of many companies with the acceleration of digital over the past 18 months: one that can deliver a competitive advantage. The good news is there's currently no shortage of budget for IT activities, says O'Donnell.

> **The CIO has gone from being someone who's very technical to someone who's about finding solutions and delivering value**

"Covid has made many boards aware of the critical importance of becoming a digital business. Across all industry sectors, this impetus to embrace a digital operating model is essential for survival," he says, pointing to areas like customer self-service.

Anna Barsby is a former CIO of Asda, Morrisons and Halfords. She's now a co-founder of Tessiant, which provides access to senior executives who can guide businesses through key stages of transition.

Barsby believes CIOs should be invited to board meetings where key decisions are being made.

"If organisations want the CIO to speak the CFO's language, then they need to ensure that the CIO is in the room when those business, financial and commercial conversations are taking place," she says. For example, if a CIO can explain how a technological investment will get more products on the shelves at the right time and improve sales by 10%, "this is speaking the language of the CFO."

However, many CIOs report to CFOs, she notes. This "devalues the CIO role and it's not ideal that the CIO is working for, rather than alongside the CFO. If the CIO reports in to the CFO this also creates the perception that IT is a cost centre within the business, when IT should be viewed as a profit centre, an enabler of successful business outcomes and a driver of commercial success and increased shareholder value," she explains.

CIOs can sometimes struggle to describe the impact of a requested IT budget on business performance. McGovern says he benefited from studying for an MBA and suggests CIOs familiarise themselves with the basics of finance.

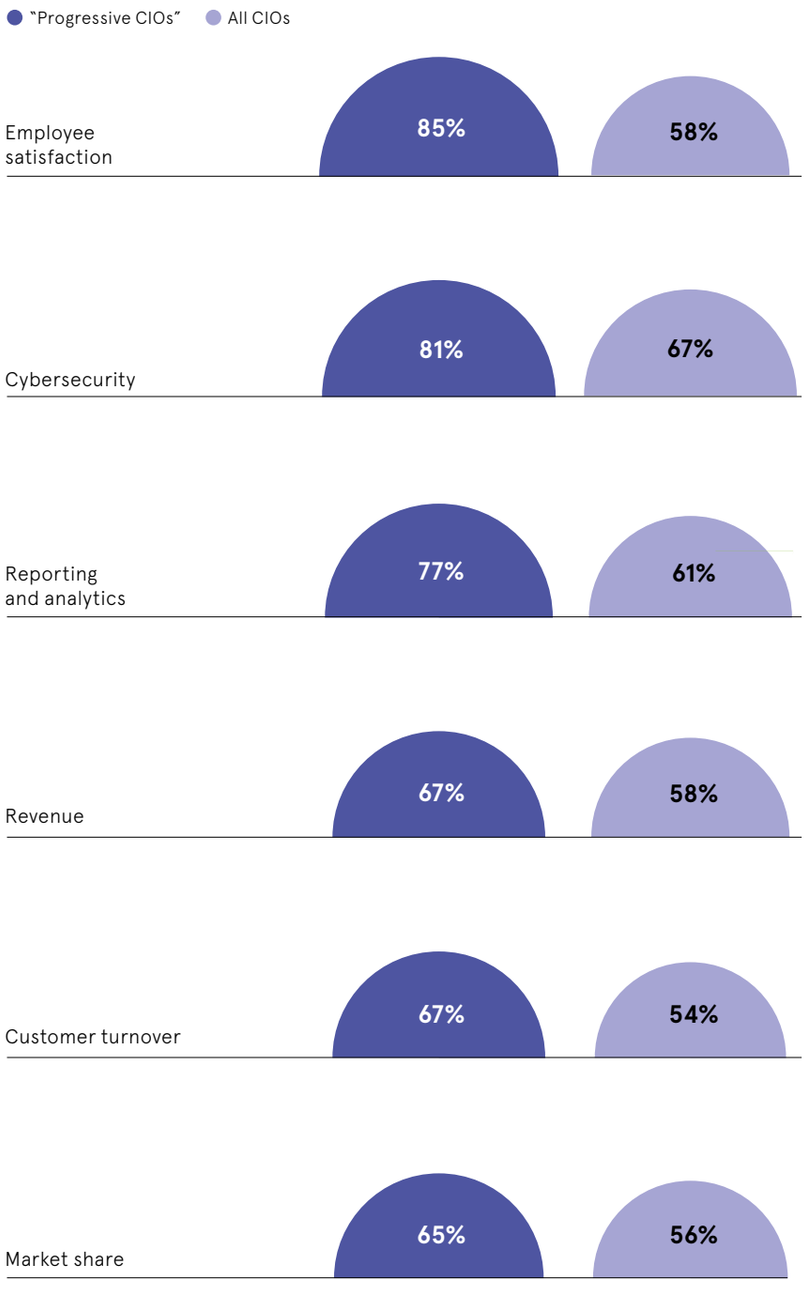
"It doesn't need to be intensive, it's just so you know the correct words, phrases, concepts that you're dealing with. You don't need to go into the minutiae of bonds, advanced finance, the risk-free rate of return – you just need to understand the basic concepts."

Ultimately, the CIO today is charged with helping to take the company to the next level through innovation. For this to happen, McGovern says the CFO should be the CIO's best friend.

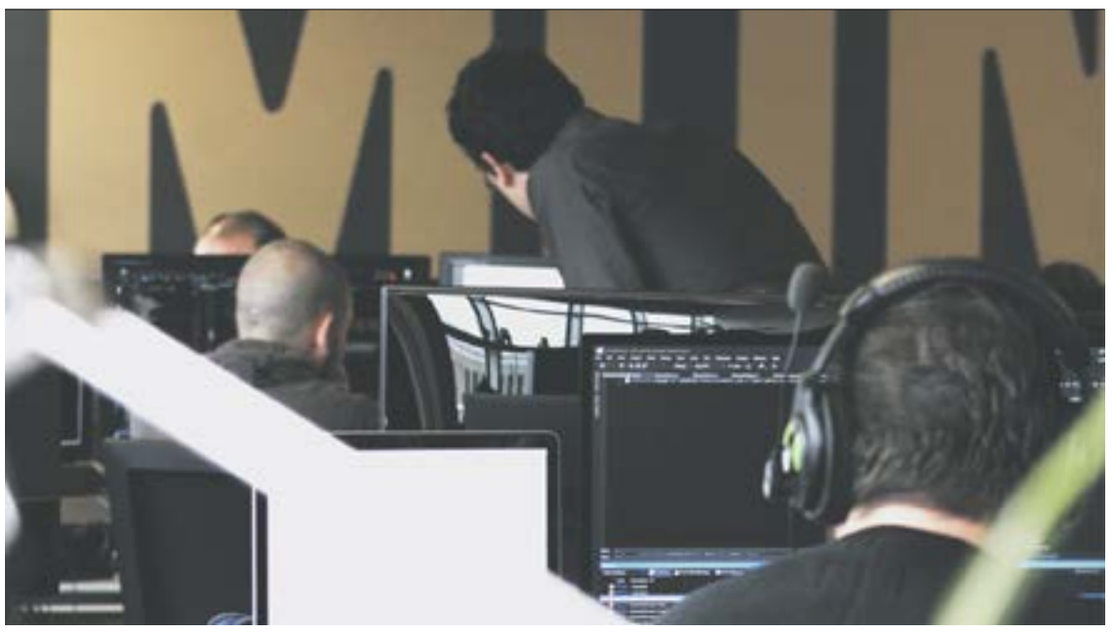
"They're the person, other than the CEO, who's going to sign the cheques and make sure that what you're doing is financially justifiable. And if you can prove that, they'll be your biggest supporter."

THE MODERN CIO KNOWS WHAT MATTERS TO THE CFO

Percentage of CIOs worldwide who say their organisations' performance increased or significantly increased in the following areas over the last 12 months



Deloitte and Workday, 2021



Closing the skills gap: how can businesses level up their cybersecurity?

Cybersecurity skills gaps are a serious issue, but external expertise and secure cloud services can help to tackle the problem

For many employees, the shift to home working has removed the need for the daily commute and created a better work/life balance. But employees are not the only ones to benefit from recent changes in the way people work.

Cyber attacks surged during the pandemic as hackers took advantage of increased digital activity, with over 5,200 data breaches confirmed globally in 2021 so far – a sharp increase on the 3,950 reported in the whole of 2020. Given that data breaches often result in significant monetary fines and severe reputational damage, no business can afford to ignore this rise in malicious activity. Yet a survey by Censuswide on behalf of IONOS Cloud, Europe's leading provider of cloud infrastructure and cloud services, found that over 40% of IT decision-makers believe their business has a cybersecurity skills gap, with a third admitting this gap is putting their organisation at risk of security threats.

Worryingly, a quarter of those surveyed also stated that their organisation is not adhering to necessary legislation. "These statistics are shocking," says Achim Weiss, CEO of IONOS. "They show how vulnerable organisations could be – both to cyber threats, and monetary fines."

While the skills gap is a clear issue, many businesses do recognise the importance of cybersecurity, with more than three-quarters of IT decision-makers from across the manufacturing, healthcare and insurance sectors saying it is either the top priority (34%) for their business or within the top three (42%).

However, when asked about cybersecurity risk assessments, there was a real disparity among the responses. Remarkably, only a third of those surveyed have conducted a threat analysis in the past 12 months, while 12% have never conducted one and don't plan to. This demonstrates a lack of understanding regarding the importance of preventative risk monitoring, which can highlight security issues so they can be addressed before an incident arises.

> **That's why it's vital companies put measures in place to plug these gaps, and don't hesitate to work with external expertise to ensure businesses are protected**

Failing to identify and resolve these issues can have catastrophic repercussions – particularly given the number of ways that data breaches can occur today. When asked to identify the biggest threats to their business, respondents cited increased DDoS attacks, phishing and scam attacks, employees downloading unapproved apps and employees storing data improperly. So why aren't businesses doing more to protect themselves from these threats?

"What's clear from the new insights is that businesses understand the importance of both cybersecurity and data protection, but missing skillsets are leaving organisations extremely vulnerable," says Weiss. "That's why it's vital companies put measures in place to plug these gaps, and don't hesitate to work with external expertise to ensure businesses are protected."

Building expertise

Despite any skills gap they might have, eight in 10 respondents to IONOS's survey still believe they are prepared to handle a cyber attack – largely due to investment in more secure cloud services.

Carefully planned and configured cloud deployments provide scalable, flexible, and secure operations for businesses. External cloud providers, working with IT teams to implement a strategy that is tailored to specific business needs, also offer an extra layer of defence and additional knowledge on ever-evolving cyber threats.

It is essential that senior leaders understand how cloud providers can positively impact data management and cybersecurity. "This awareness allows you to have more informed and considered conversations when choosing external providers, allowing you to work with IT leads to put effective, cohesive strategies in place," says Weiss.

As well as employing the right external expertise, senior leaders must also work closely with their teams to identify where cybersecurity knowledge gaps exist and create a plan to address them. In fact, a third of those surveyed said that because senior leadership had put more focus on cybersecurity, they felt more prepared to handle a cyber attack.

In addition, "IT teams must feel confident and trust that senior leaders will listen when they raise concerns on how skills gaps are impacting the business," says Weiss. Biannual planning meetings can provide an opportunity to review skills across the business and get this conversation flowing. Once gaps have been successfully identified, staff can then be upskilled – or new team members hired – to plug them.

It's important that senior leaders also show a willingness to learn new skills themselves. "Engaging and taking an interest in understanding the impact and possibilities of new tech on the business will show teams that this is a business issue you're taking seriously," Weiss explains.

Data protection

Strong security procedures are essential for adhering to increasingly strict data protection laws. Nearly 60% of businesses surveyed said they are putting more focus on adhering to data protection, compared to before the pandemic. However, 13% are actually giving it less attention, with almost half of these citing time pressures and workload as the main reasons why they struggle to ensure the business is up-to-date with the latest legislation.

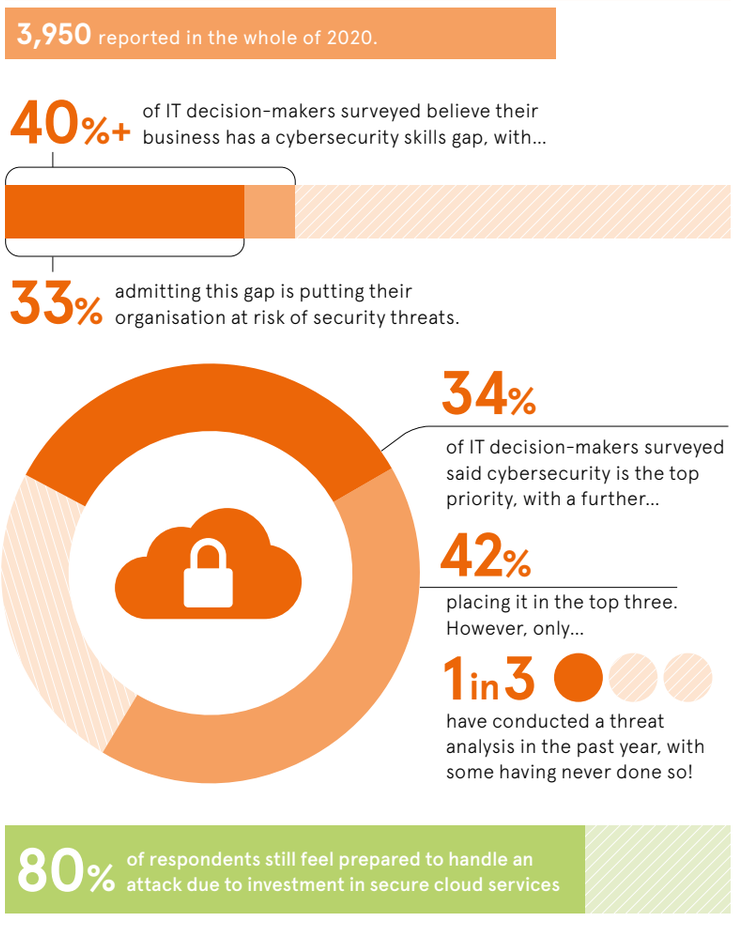
Although time constraints are understandable while businesses deal with fallout from the pandemic, few of them can afford to let data protection take a backseat. Indeed, with the Information Commissioner's Office setting significant monetary fines for breaches to GDPR law, businesses must ensure they are fully aware of compliance procedures and the latest legislative requirements when handling personal data.

"When it comes to data protection, action must be taken to bridge knowledge gaps," says Weiss. "IT teams are under great pressure to adhere to the latest legislation, but one way to help minimise risk when it comes to data is to work with European-based cloud providers that adhere to GDPR – rather than those that must also work under laws such as the US CLOUD Act."

Any successful solution to the cybersecurity skills gap must also involve everyone in the business – not just overstretched IT teams. As Weiss says, "While factoring in improved software with better cybersecurity measures is a sound way to protect the business at a strategic level, having open dialogue with employees across all levels means cybersecurity and data protection knowledge is shared and best practices are front of mind at all times."

CYBERSECURITY SKILLS GAP WIDENING IONOS, 2021

Remote working and onboarding may leave companies more vulnerable to cyber attacks



Commercial feature

Operational resilience now key to organisational success

Operational resilience is key to success in digital transformation. Speakers at a recent roundtable shared their expertise on organisational change

Nick Easen

At no point in history has our dependence on digital services been so high, at the same time, our tolerance of poor IT systems, security, data-driven workflows and connectivity has never been so low. The Covid pandemic has also accelerated the pace of change with business transformation projects at full throttle. This has sparked many to reimagine their organisations as digital-first.

In the process, businesses are trying to become more agile, empower themselves with vast amounts of actionable data, while consolidating and rationalising their IT infrastructure. All of these manoeuvres, which are happening at once, are putting extraordinary pressures on the technical C-suite and their teams – making operational resilience a hot topic.

The term means many things to many organisations, but the ability of IT systems to run unhindered, cope with change, react and act intelligently, deal with cyberthreats and drive business outcomes are now vital goals for many. Operational resilience therefore becomes synonymous with success. Get it right and it allows decision makers to learn from the past, deal with the present and plan for the future.

"Operational resilience is the ability to quickly and decisively cope with fast moving or unseen changes that cannot be avoided. If there's anything we've seen over the past two years, having that capacity to absorb some of those unseen changes and to keep things moving for businesses is important," said Mark Woods, chief technical advisor at Splunk.

The opposite of operational resilience is vulnerability, which can be costly. Roblox, a popular global video game, which recently experienced a tech outage, lost $1.7bn in three days, close to 47 million people use it. Facebook's seven-hour outage cost millions of dollars, wiping 5% off its share price. The costs are eye-watering, yet resilience requires investment and new thinking.

"We look at resilience through the three Ps – people, process, and platforms – and in that order," said Shez Partovi, chief innovation and strategy officer at Philips. "We also see it through the lens of predicting the future."

Vulnerability equals cost

The ability to monitor the three Ps using data and tech are increasingly vital for organisations. It is allowing them to take decisive action. This will determine whether businesses thrive in the future. At the same time, we're at a tipping point in terms of our dependence on IT to deliver; this is occurring across sectors, whether it's financial services, healthcare or telecoms.

"Our IT systems are becoming utterly integral to how we deliver care," said Mark Reynolds, interim chief technology officer at NHS Digital. "When a service is unavailable, care suffers. Operational resilience is making sure our systems and services are always available, and always operational."

The fact is systems do go down, climate-induced floods in Germany earlier this year forced Deutsche Telekom to re-evaluate its resilience; 50,000 customers were impacted, some customers died. "We completely lost our mobile and fixed line telecoms. This gave us a kick to prioritise operational resilience because it was down to our infrastructure. The flood was completely unseen. We are expecting much more in the future with climate change. This gave us a new priority," said Nils Stamm, chief digital officer for Deutsche Telekom.

Complexity can be a challenge

Businesses need to digitally transform and constantly evolve which can make it challenging to achieve operational resilience. Organisations need to make the most of their data to break down siloes, consolidate and simplify IT systems, whilst enabling the spread of tech-driven architectures to more business units. Decision-makers also need to factor in ageing IT stacks, siloed and new functions in this drive toward agility.

> **You can have amazing processes and platforms, but if people, both inside your organisation and people you are interacting with, like clients and external stakeholders, don't understand the purpose and use of the technology you are implementing, then you will have real challenges**

"Legacy systems are an issue, while those people that manage them are close to retirement. We have 150-200 systems working together to deliver each country's banking offering. It is very difficult, you want to change all of this at speed. You want all this to be digitally enabled. You simply cannot change that much, that fast," added Tommy Flynn, chief operating officer for wholesale and rural at Rabobank.

In the past, understanding across IT and business units has been difficult to connect and share. With significant digitalisation over the last few years, the opportunities for business-led insight have vastly increased. Whilst oversight is now potentially easier, critical functions like security still need to address evolving concerns.

"We are seeing a backdrop of increasing complexity when it comes to cyberattacks with multiple countries, publicly saying they're developing their cyberpower," said Mary Haigh, chief information security officer at BAE Systems. "Knowing the networks you've got to protect and being aware of the types of attack that come in and being ready for one on the scale of SolarWinds, that we've not predicted before is vital."

Mass migration to the cloud also makes it possible to deploy state-of-the-art systems and applications at affordable prices. Yet this in turn creates new challenges. "Once you migrate to the cloud and you are dealing with evergreen IT systems. They become difficult to keep up with. Evergreen systems are continually evolving. Therefore, one thing we've been looking at is embracing open source," said Gissur Simonarson, senior domain architect for Fujitsu.

Another factor widely talked about is the people aspect, when it comes to delivering resilience. Organisations need to upskill staff alongside deploying technology. "You can have amazing processes and platforms, but if people, both inside your organisation and people you are interacting with, like clients and external stakeholders, don't understand the purpose and use of the technology you are implementing, then you will have real challenges. We want people to be resilient, agile and adapt to changing technologies," said Kimberly Morris, chief people, technology & operations officer at Fifa.

Free up time for innovation

For businesses the ability to see connected risks and opportunities, make decisions and respond has never been more important. This is what should be driving investment. It allows corporations to be proactive, they can continually improve, collaborate across the organisation, achieve agility and drive outcomes in real-time.

"Operational resilience now allows you to do corporate strategy on steroids, you don't have to wait for that five-year program. You've got the information, you know what's happening in the outside world, you can shift the operation. So, you can move forward quickly. Speed and agility – that's what it means to us," said Sandra Bell, group head of organisational resilience at Hitachi Capital UK.

Once organisations achieve better operational resilience, it will allow them to focus on what they do best – their core business. This is likely to drive further investment.

"If you have less firefighting you have freed up time, you can free up human brain power to leverage technology and data to drive innovation, to develop new products and new business models, which then have a bigger impact on society," said Amit Nastik, global Head for strategy and operations and local markets manufacturing at Novartis. "Today resilience is key to future innovation."

INTERVIEW

NCSC chief tackles a bulging cyber threat in-tray

As head of the National Cyber Security Centre, **Lindy Cameron** believes company leaders must improve preparedness and resilience by educating staff – and themselves

Oliver Pickup

Lindy Cameron is a difficult person to reach. That's understandable: as CEO of the National Cyber Security Centre (NCSC), she's at the forefront of the UK's fight against computer security threats. While it's tough for a journalist to negotiate an interview, it's reassuring that she's dedicated to her task.

The NCSC provides advice and support for both public and private sector organisations, helping them avoid computer security threats. Cameron took the helm in October 2020, succeeding inaugural CEO Ciaran Martin, who stepped aside after four years in the job.

Her assessment of cyber threats, themes and advice should be required reading for CIOs and other members of the C-suite. Indeed, on the rare occasions she has spoken in public since taking up the role, she hasn't held back.

For instance, in March she warned of the UK's need to be "clear-eyed about Chinese ambition in technological advancement". Speaking in her first address as CEO, she chided China's "hostile activity in cyberspace" while adding that "Russia [is] the most acute and immediate threat" to the country.

The former number two at the Northern Ireland Office has over two decades of experience working in national security policy and crisis management. She was equally forthright and insightful in October's keynote speech at Chatham House's Cyber 2021 conference, where she reflected on her first year at the NCSC and identified four key cybersecurity themes. The most alarming is the pervasiveness of ransomware, the scourge of business leaders.

In May, US cloud-based information security company Zscaler calculated that cybercrime was up 69% in 2020. Ransomware accounted for over a quarter (27%) of all attacks, with a total of $1.4bn demanded in payments. And those figures didn't include two hugely damaging breaches that occurred in 2021, marking an elevated scope for bad actors.

July's ransomware attack on multinational remote management software company Kaseya affected thousands of organisations and saw the largest ever ransomware demand of $70m. The REvil ransomware gang that claimed responsibility for the attack ordered ransoms ranging from a few thousand dollars to multiple millions, although it's unclear how much was paid. The gang said 1 million systems had been impacted across almost 20 countries. While those numbers are likely to be exaggerated, the attack triggered widespread operational downtime for over 1,000 companies.

The Kaseya incident came two months after the attack on Colonial Pipeline, one of the largest petroleum pipelines in the United States. The attack disabled the 5,500-mile system, sparking fuel shortages and panic buying at gas stations. Within hours of the breach, a $4.4m ransom was paid to DarkSide, an aptly named Russian hacking group. Despite the payment – which was later recovered – the pipeline was down for a week.

> **Organisations can prevent the vast majority of high-profile cyber incidents we've seen following guidance we have already issued**

"Ransomware presents the most immediate danger to the UK, UK businesses and most other organisations – from FTSE 100 companies to schools; from critical national infrastructure to local councils," Cameron told the October conference. "Many organisations – but not enough – routinely plan and prepare for this threat, and have confidence their cybersecurity and contingency planning could withstand a major incident. But many have no incident response plans, or ever test their cyber defences."

The sheer number of cyber attacks, their broader scope and growing sophistication should keep CIOs awake at night. The latest Imperva Cyber Threat Index score is 764 out of 1,000, nearing the top-level "critical" category. Other statistics hint at the prevalence of cybercrime in 2021: some 30,000 websites on average are breached every day, with a cyber attack occurring every 11 seconds, almost twice as often as in 2019.

Cybersecurity organisation Mimecast reckons six in 10 UK companies suffered such an attack in 2020. In her *Raconteur* interview, conducted a fortnight after her appearance at Chatham House, Cameron reiterated her concerns.

"Right now, ransomware poses the most immediate threat to UK businesses, and sadly it is an issue which is growing globally," she says. "While many organisations are alert to this, too few are testing their defences or their planned response to a major incident."

Despite the headline-stealing attacks, businesses aren't doing enough to prepare for ransomware attacks, says Cameron. Cyber risks can and must be managed and mitigated. To an extent, CIOs and chief information security officers (CISOs) are responsible for communicating the potentially fatal threat to various stakeholders.

Cyber attacks are different from other shocks as they aren't readily perceptible. They are deliberate and can be internal and external. They hit every aspect of an organisation – human resources, finance, operations and more – making them incredibly hard to contain.

"The impact of a ransomware attack on victims can be severe," Cameron continues, "and I've heard powerful testimonies from CEOs facing the repercussions of attacks they were unprepared for. Attacks can affect an organisation's finances, operations and reputation, both in the short and long term."

CEOs can't hide behind their security teams if breached by a cyber attack. Cameron warns that defending against these incidents can't be treated as "just a technical issue" – it's a board-level matter, demanding action from the top.

"A CEO would never say they don't need to understand legal risk just because they have a General Counsel. The same applies to cybersecurity."

Cybersecurity should be central to boardroom thinking, she adds. "We need to go further to ensure good practice is understood and resilience is being built into organisations. Investing resources and time into putting good security practices into place is crucial for boosting cyber resilience."

Cameron notes that the NCSC's guidance, updated in September, will reduce the likelihood of becoming infected by malware – including ransomware – and limit the impact of the infection. It also includes advice on what CIOs, CISOs and even CEOs should do if systems are already infected with malware.

Cameron, who was previously director general responsible for the Department for International Development's programmes in Africa, Asia and the Middle East, echoes Benjamin Franklin's famous maxim: "By failing to prepare, you are preparing to fail."

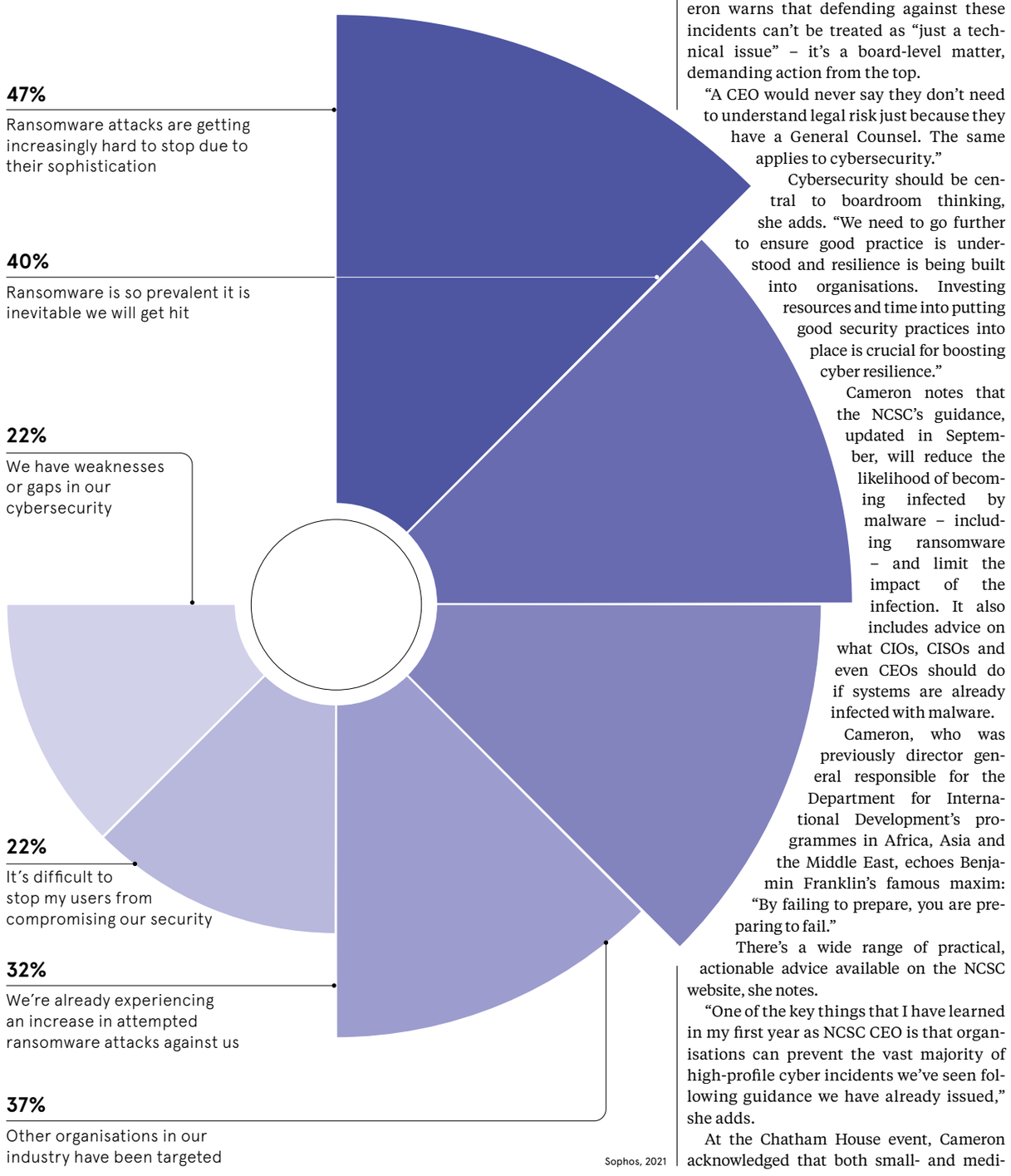
There's a wide range of practical, actionable advice available on the NCSC website, she notes.

"One of the key things that I have learned in my first year as NCSC CEO is that organisations can prevent the vast majority of high-profile cyber incidents we've seen following guidance we have already issued," she adds.

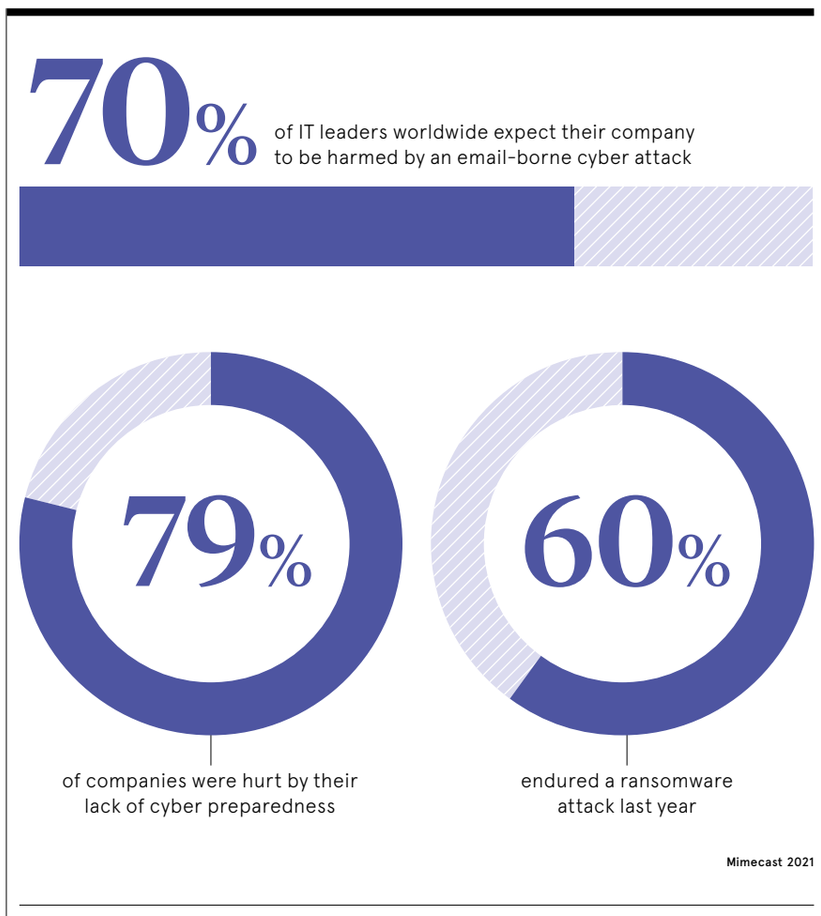
At the Chatham House event, Cameron acknowledged that both small- and medi-

CYBER ATTACKS NOW CONSIDERED INEVITABLE

Percentage of global IT decision-makers, whose companies have not been hit by ransomware in the past year, who say the following are the reasons why they expect to suffer an attack in the future



Sophos, 2021



um-sized enterprises are particularly vulnerable to cyber attacks. "I completely understand this is getting harder, especially for small businesses with less capability," she said. "But it is crucial to build layered defences that are resilient to this."

SMEs are the low-hanging fruit for cybercriminals, as they usually don't have the budget or the access for sufficient IT support or security. "We appreciate smaller organisations may not have the same resources to put into cybersecurity as larger businesses," Cameron says.

The NCSC has produced tailored advice for such organisations in its Small Business Guide. This explains what to consider when backing up data, how to protect an organisation from malware, tips to secure mobile devices and the information stored on them, things to bear in mind when using passwords and advice on identifying phishing attacks.

Criminals will seek to exploit a weak point, which could include an SME in a supply chain. Larger organisations, says Cameron, have a "responsibility to work with their suppliers to ensure operations are secured. In the past year, we have seen an increase in supply chain attacks with impacts felt around the world, underlining how widespread supply networks can be."

Supply chain attacks were another of Cameron's four key themes at the Chatham House conference. Such vulnerabilities "continue to be an attractive vector at the hand of sophisticated actors and... the threat from these attacks is likely to grow," she said. "This is particularly the case as we anticipate technology supply chains will become increasingly complicated in the coming years."

The most infamous recent supply chain attack was on SolarWinds, said Cameron. According to the former CEO and other SolarWinds officials, the breach happened because criminals hacked a key password – it was solarwinds123. This highlights the importance of strong passcodes for companies large and small.

"SolarWinds was a stark reminder of the need for governments and enterprises to make themselves more resilient should one of their key technology suppliers be compromised," Cameron said at Chatham House.

The two other areas of cyber concern she promoted were the vulnerabilities exposed by the coronavirus and the development of strategically important technology. "We are all increasingly dependent on that technology and it is now fundamental to both our safety and the functioning of society," she said of the latter.

> **Staff can be an effective first line of defence against cyber attacks if they are equipped with the right understanding and feel they can report anything suspicious**

On the former theme, Cameron said that malicious actors are trying to access Covid-related information, whether vaccine procurement plans or data on new variants.

"Some groups may also seek to use this information to undermine public trust in government responses to the pandemic. The coronavirus pandemic continues to cast a significant shadow on cybersecurity and is likely to do so for many years to come."

CIOs must keep this in mind as many organisations grapple with post-pandemic ways of working. This involves more remote workers using personal or poorly protected devices on unsecured networks, all of which play into the hands of bad actors.

"Over the past 18 months, many organisations will have likely increased remote working for staff and introduced new online services and devices to stay connected," says Cameron. "While this has offered a solution for many businesses, it's vital for the risks to be mitigated so users and networks work securely. Our home-working guidance offers practical steps to help with safe remote working."

Providing other essential advice, Cameron underlines the importance for organisations of all sizes to build up their cyber resilience significantly.

"It's vital that organisations of all sizes take the right steps to build their cyber resilience. Educating employees is an important aspect of keeping any business secure. Staff can be an effective first line of defence against cyber attacks if they are equipped with the right understanding and feel they can report anything suspicious."

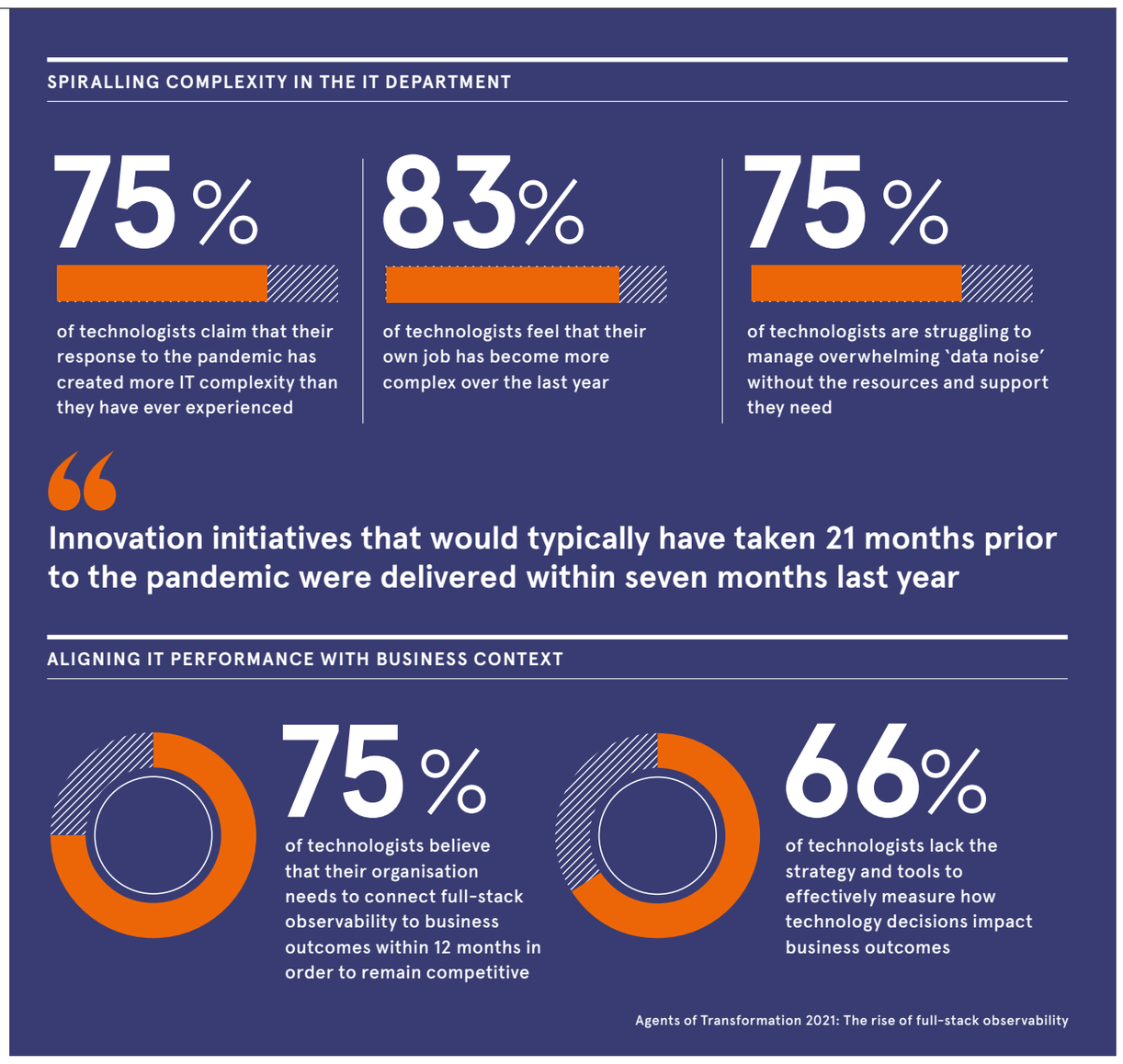
Businesses should put a clear IT policy in place that guides employees on best practices, while staff should be encouraged to use the NCSC's "Top Tips for Staff" training package.

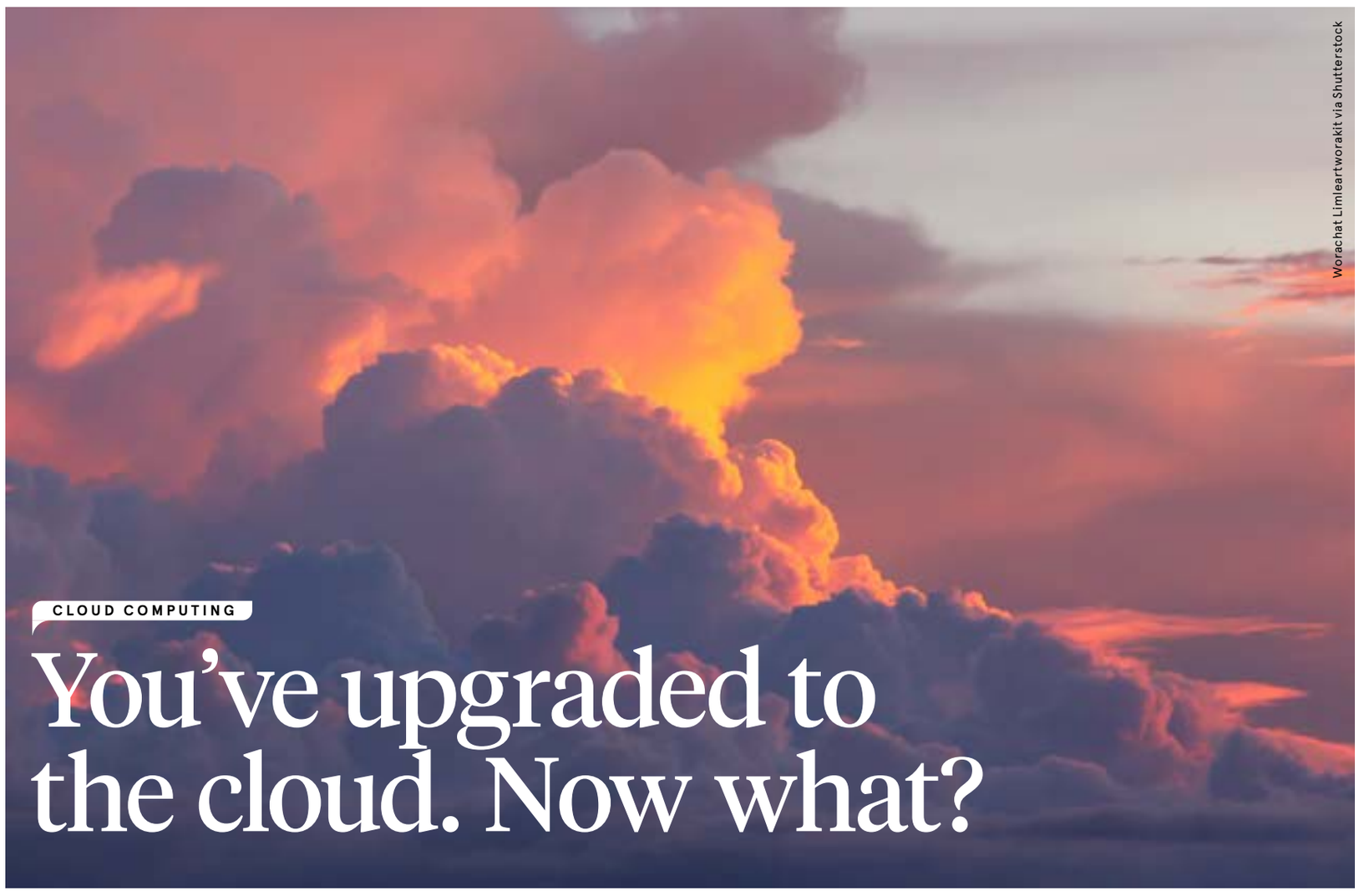
"These steps are about creating a positive cybersecurity culture and we believe senior leaders should lead by example," she adds.

The NCSC's Board Toolkit is particularly useful for CIOs, designed to help facilitate cybersecurity discussions between board members and technical experts. It will "help ensure leaders are informed and cybersecurity considerations can be integrated into business objectives".

These conversations are now critical, as advances in artificial intelligence, the internet of things, 5G and quantum computing multiply attack surfaces. Reflecting on the NCSC's work since its inception five years ago, Cameron says the organisation has achieved a huge amount, including dealing with significant cyber incidents, improving the resilience of critical networks and developing a strong skills pipeline for the future.

"This is delivering real benefits for the nation, from protecting multinational companies to defending citizens against online harm. However, the challenges we face in cyberspace are always changing, so we can't rest on our laurels."





Worachat Limleartworakit via Shutterstock

CLOUD COMPUTING

You've upgraded to the cloud. Now what?

Shifting to the cloud is no mean feat, but success depends on what comes next. CIOs must balance technical demands with training needs

Andy Jones

Any experienced sailor knows it's easy to launch a vessel – the hard part is keeping it afloat once you're out at sea. The same can apply to chief information officers (CIOs) who've successfully upgraded their business to the cloud.

Finding your sea legs quickly as wave after wave of problems hit – including creaking legacy technology, belligerent employees and the ever-present threat of cyber attacks – is key to post-cloud survival.

Helen Ashton helped power fashion giant ASOS through several technological shifts, moves which ultimately made them the market leader in online shopping, earning £3.26bn last year. Now founder of Shape Beyond, a business transformation consultancy, Ashton says the key to success at ASOS was full migration to the cloud.

However, new technology only brings the expected benefits when people are kept on board with the processes needed for success.

"Businesses either plan for months in minute detail or they jump straight in to work on the sexy stuff, such as analytics or digital CX," says Ashton. "But success comes from winning hearts and aligning incentives. It is amazing how easily focus can shift through overzealous project management to ticking off activities on the plan rather than keeping sight of delivery of the outcomes identified as indicators of success."

You can use some of the cloud's metrics and data to demonstrate quick wins and progress. However, the key to ongoing cloud success is to share data in a way that empowers staff to problem-solve within the business, creating a sense of shared responsibility that allows all parties to see bottlenecks and show who needs help and why, says Ashton.

Before you share all your data internally, make sure a hole in your S3 bucket isn't sharing it everywhere else.

A simple S3 bucket exposure from an unknown public source leaked personal details of 120 million Brazilians – including banks, credit details and voting history – partly because an administrator had renamed the index.html by accident. In separate examples, a mobile app developer exposed 500,000 documents from a finance app and a cannabis retailer leaked 30,000 of its customers' details, which all led to considerable fallout and organisations falling foul of data privacy regulations.

"We've seen incidents on a frequent basis where cloud databases have been set to be publicly accessible, when they needed to be private," says Javvad Malik, lead security awareness advocate at KnowBe4. "Similarly, having the appropriate authentication controls in place is vital to prevent account takeovers which exploit weak credentials."

To prevent leaks, look for gaps where cloud migration shifts data centre responsibility from the traditional sysadmin to site reliability engineers and DevOps teams, says Tim Mackey, principal security strategist at Synopsys Cybersecurity Research Center. "This shift creates a potential gap between those familiar with the application security requirements and those versed in cloud security topics. This can lead to situations where storage misconfigurations in the form of unsecured S3 buckets result in significant data leakage."

Patch management is also an area of risk, particularly when long-running servers are upgraded but containerised microservices haven't been redeployed, says Mackey. "If the pre-existing patch compliance dashboard was based on logging into all systems, it will need to be updated for a containerised deployment."

While you're taking the lead, your team can only follow if they've been trained correctly. In the haste of initial deployment deadlines, the required level of understanding is often lacking across the team, says Mackey. While this should be remedied with training, security access should be kept on a need-to-know basis, not just given to those at senior levels, even if that requires diplomacy.

"Training efforts should focus on how to operate a cloud service using principles of least privilege. Once training is complete, a comprehensive review of gaps in implementation should be performed and any issues remediated."

While not everyone needs access, staff should still be aware of all security settings and why they're in place, with drill tests to ensure all such settings are as they should be. "A culture of security needs to be built that understands the risks of the cloud," says Malik. "Use internal and external data sources to determine the root causes for most attacks against cloud infrastructure, and invest in the appropriate human, procedural and technical controls."

It's also important to know when to hand over control to the system. If you don't automate quickly it can create sluggish staff, put off new hires and create extra labour and therefore costs.

"If you don't automate, organisations become less agile or adaptable to change and teams may also demotivate because of repetitive tasks," says Sergio Loureiro, cloud security director at Outpost24, a cybersecurity specialist. "Today, when it is hard to find a skilled workforce, automation is a competitive advantage. Finally, customer perception can be impacted by longer response times."

Despite all the technological risks, many problems will come from humans. Even at ASOS, human nature states people always want to keep the status quo, says Ashton. "In more traditional businesses, there is a strong possibility of 'adoption indigestion,' which can derail cloud's anticipated benefits if not effectively managed. There is no silver bullet solution here. It is a mix of training, communicating the benefits, real-time support, and measuring process and outputs to identify issues and successes."

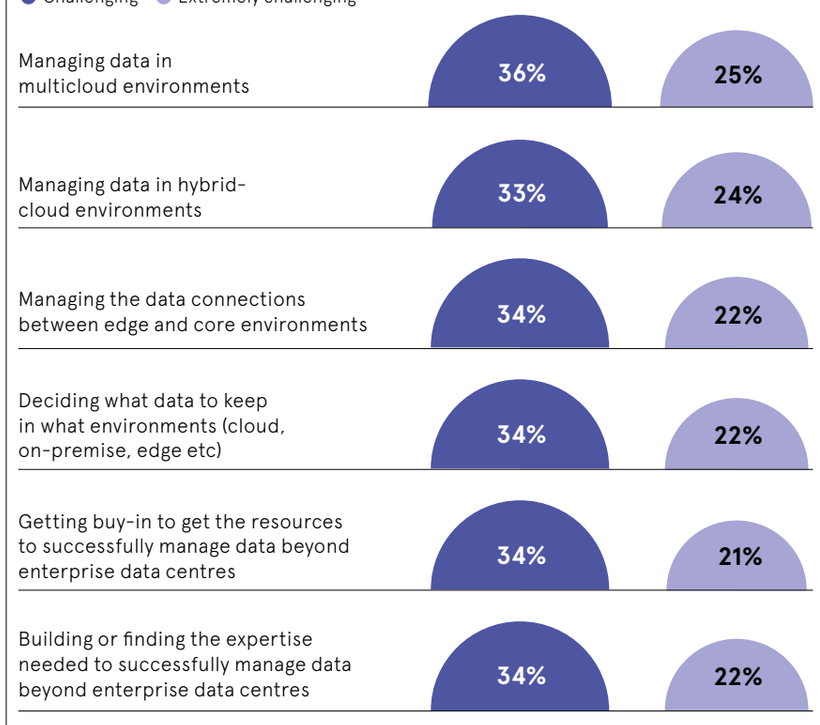
While cloud software does a lot of the work for you, keep peace of mind by inviting occasional outside input, says Andrew Whaley, senior technical director at Promon, white hat hackers that test large-scale organisations. "Businesses still need to check that security has been applied correctly. Periodic assessments by third party pen testers is a good way to check this."

Testing how watertight your vessel is inside and outside of the water, while ensuring all those on deck understand the direction of travel, is key to charting a clear and positive course for your business on the cloud.

TOP CHALLENGES ONCE YOU'VE MOVED TO THE CLOUD

Percentage of IT leaders worldwide who said the following activities would be "challenging" or "extremely challenging" over the next two years

Seagate and IDC, 2020

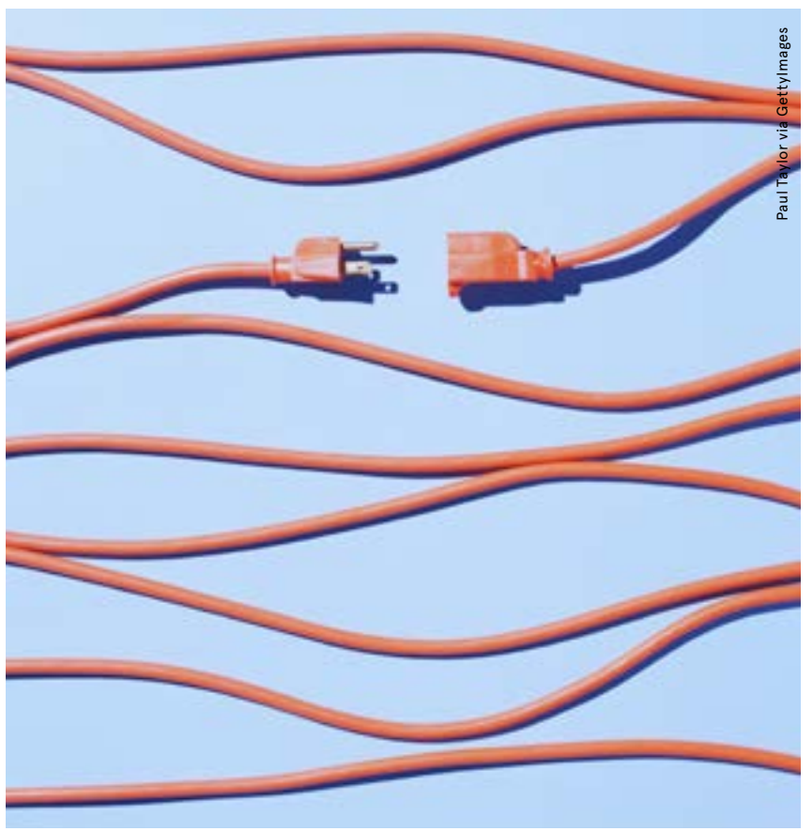


CYBERSECURITY

Air gapping: the ultimate in cybersecurity

Worried about viruses? Maybe you should disconnect your entire system

Charles Orton-Jones



Paul Taylor via GettyImages

A major food company in the Midlands found a simple way of avoiding ransomware and viruses: it disconnected the factory IT system from the internet. No connection, no attackers.

This approach is known as "air gapping". With no physical link to the outside world, the IT stack is isolated. Security guaranteed, in theory. But is it a viable strategy?

Government agencies like the CIA in the US have started to recommend air gapping as part of a comprehensive anti-ransomware programme, notes Joe Sullivan, chief security officer at website security specialist Cloudflare.

"Air gapping has existed as a security and resiliency concept in business continuity programmes since well before the term 'ransomware' became popular," he says. "It has typically been used as a way to protect against accidental or malicious destruction of primary sources of data and software by making backup copies that are stored offline."

Air gapping grew in the aftermath of the high-profile attacks on the likes of Saudi Aramco and Sony, which used software like the Shamoon wiper virus to erase sensitive data.

Today, the urge to unplug is soaring. The FBI warns there are more than 100 strains of ransomware circulating. In the second quarter of this year there were more than 300 million attempted attacks captured by a single security provider, more than the whole of 2020. Payouts in 2021 should top the entire past decade put together.

However, there are good reasons why air gapping is still niche. As Sullivan notes: "There is an old joke in security that a computer is only safe when it is turned off. Sadly, that has been proven true. Every system that is powered up and online is under threat."

One major problem with air gapping is that systems can't be updated easily. Software updates get skipped. The system grows vulnerable.

"When systems are air gapped the priority of investing into the implementation of proper security controls goes away," says Ehsan Foroughi, CTO at Security Compass. "System developers get too relaxed and start relying on that air gap as their defence."

Sooner or later an upgrade must be made. The system connects to the outside world and exposure returns, only worse than before. The unprotected system is vulnerable, missing months or years of upgrades and security patches.

There is also the issue of human error. Foroughi tells the story of a US government network behind an air gap that was compromised because one employee found it too hard to keep replicating work between two desktops, one connected to the air gap network and one to the internet. So, he temporarily connected them, breaking the air gap – thereby allowing attackers to jump across the bridge into the protected network.

There is another problem. Perhaps surprisingly, it turns out that a disconnected system may not be isolated after all.

> **There is an old joke in security that a computer is only safe when it is turned off. Sadly, that has been proven true**

Mordechai Guri is an academic researcher at Israel's Ben-Gurion University of the Negev and an expert at hacking unconnected systems. In a recent paper he revealed how he could read the signals from an ordinary ethernet cable using a $1 antenna. The cable electrically leaks information, which can be read from up to tens of metres away. He was also able to transmit information.

Guri's method requires a direct physical attack on an IT system, hence Russian ransomware villains may be unlikely to try it. But Guri has found around a dozen other ways to connect to air-gapped systems by picking up leaked signals. One of his methods involves analysing the acoustic waveform emitted from the CPU and chassis fans to transmit information, captured on a nearby mobile phone at 900 bits an hour – slow, but usable.

The only solution to this snooping is to keep attackers at a physical distance or install a Faraday cage, which blocks electromagnetic transmissions. Even then, a physical attack is possible. Hackers may break into a facility and upload malware via a USB stick. The Iranian national nuclear programme is believed to have been compromised this way – it was an air-gapped system.

Air gapping also faces a challenge from alternative methods of protection. Zero Trust networks for example, offer elevated security with few of the downsides. In a Zero Trust environment only a limited set of approved devices can connect. Access is limited by time. Users can access only a narrow subset of systems. The philosophy is based on the assumption that each access could be a malefactor; it sets out to limit the blast radius inside the internal network.

There are also One Way Links, using network diodes. These allow data to travel only one way through a system. "Unidirectional communication could allow you to collect data from a secured, usually air-gapped place like a nuclear power plant," says Steve McGregory, senior director, security R&D at Keysight Technologies. "This would prevent someone from being able to connect into the nuclear power plant through that connection."

So what's the future for air gapping?

The inability to update air-gapped systems means they grow ever weaker. The chances of an accidental connection or rogue breach of the gap are unpalatable. And naturally, a disconnected system is limited in its capability. No emails, no upgrades, no data sharing with the outside world: it's a high price to pay.

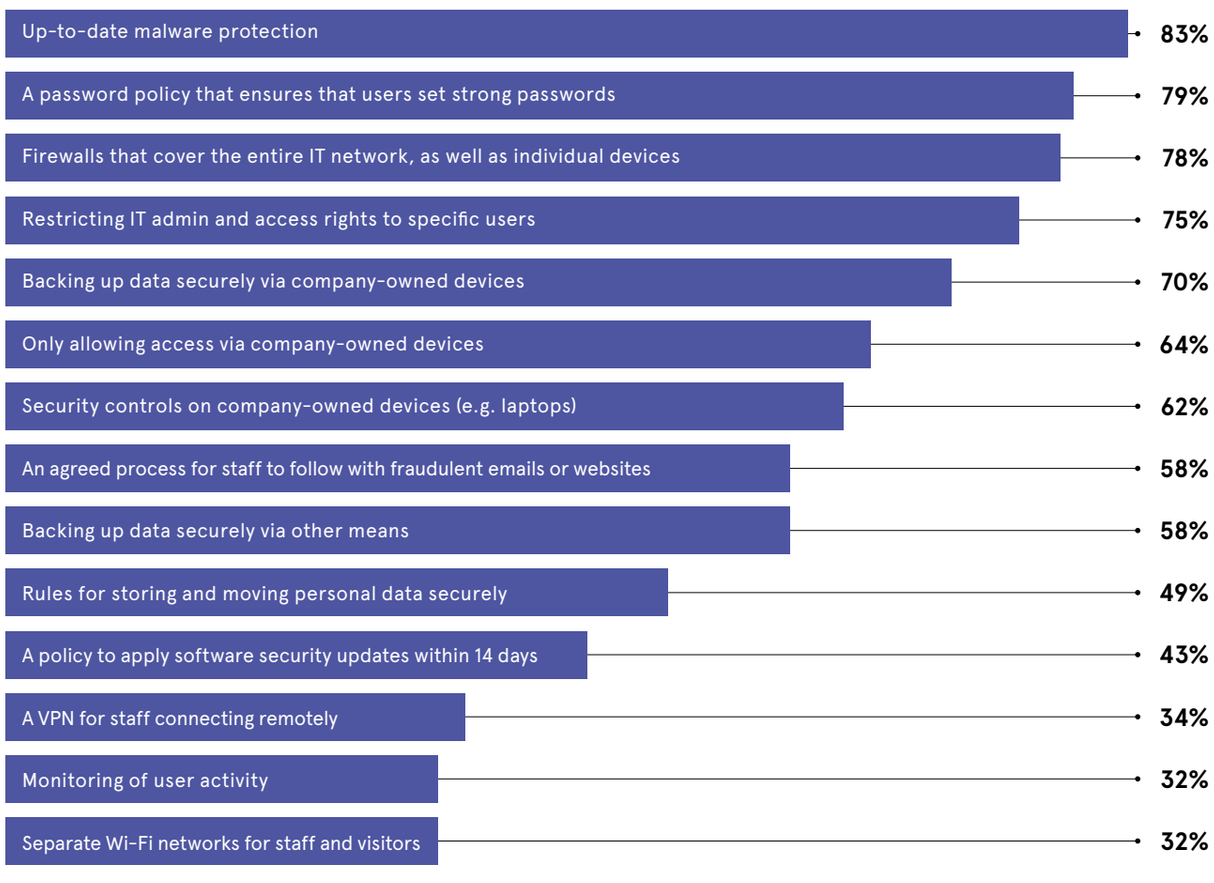
But there is a use case. Backups are vital in combating ransomware, when infected systems need to be restored. However, malware will seek out and infect backups. A simple method to protect them is to place them in an air-gapped storage unit. Laborious, yes, but secure.

"Air gapping is the only real defence against ransomware, which continues to offer the biggest threat to information systems," says Tony Proctor, principal lecturer in cybersecurity at the University of Wolverhampton. "Many organisations have kept their backup systems online for convenience when copying the live data. As such they are highly vulnerable to ransomware. Air gapping means that these backups can be maintained offline and will not be affected by the ransomware."

As ransomware gangs like Evil Corp (yes, that is its name) run rife, air gapping backups may be the solution. It's not perfect. It's labour intensive. But when disaster strikes, it may prove to be the low-tech solution that saves the company.

AIR GAPPING NOT CURRENTLY COMMON PRACTICE

Percentage of UK businesses who say that they have the following cybersecurity rules or controls in place



Department for Digital, Culture, Media & Sport and Ipsos MORI, 2021

Commercial feature

Assume breach in the hybrid working age

Security leaders from across sectors joined a roundtable this month to discuss the new realities of cyber risk in a hybrid working world where breaches must now be assumed

Ben Rossi

It is now clear the end of the pandemic will not see a return to the working models of the past, as organisations work on designing new hybrid working practices. Exactly how that is defined differs from company to company. For the security experts who participated in this roundtable discussion, it's the cyber risk implications of this shift that matters most.

The pandemic meant the need to access data at all costs, remotely and via the cloud, was suddenly a matter of business survival. In many companies, it even changed the perception of what data is, as the mindset of security departments evolved from needing to secure all endpoints, servers and devices, to recognising a new reality where the device is merely the place where the data sits. The true value is in the data. And even then, the question is no longer just what data is where, but who's using it, what for and how much are they trusted?

In terms of core infrastructure, even before the pandemic many enterprise organisations were already treating all employees as remote workers, on the cloud, regardless of where they worked. When the perimeter suddenly extended to people's bedrooms and lounges, however, it exposed the void between technology and culture. With workers likely to be more relaxed, perhaps even careless, when at home, the Covid-19 crisis has presented an urgent need for more persona-based activity around data access, as well as a strong mindset shift driven by education about threats, behaviours and vulnerabilities.

"The perimeter model has been dead for years and arguably so is the model of locking things down," says roundtable panellist Joseph Da Silva, CISO at Electrocomponents. "We now must assume breaches will happen. Things will go wrong and our stakeholders need to understand we won't be able to fix everything because this is a risk game. The key now is how do you respond to it and are you prepared? At the moment most of our security models are built from a technology perspective, how do you prevent X and Y? The user is typically a much lower consideration. Cybersecurity has got to become much more human centric at the design stage."

Achieving that human centricity means building security around humans, not the other way around, and striking the appropriate balance between a frictionless user experience and keeping a necessary level of security and least privilege. It's a tricky subject, not least because CISOs are keen to now be seen as enablers, not blockers, to the wider business.

Education can minimise human error but not eliminate it altogether, so security measures must still be robust. Equally, however, if users reject a process, it becomes unusable, and constantly prompting employees to prove who they are can soon cause authentication fatigue. Again, getting the right balance requires a different mindset, adopting the thought processes of attackers to think about their lateral movement once they have gained access.

"Once you assume they're in, it changes the way you think about how to protect the business, and you end up protecting from the inside out rather than the outside in," says David Higgins, EMEA technical director, CyberArk. "Meanwhile there are things we can do in terms of striking that balance. A lot of consideration has to be had around identities and how they're used consistently but also securely whilst maintaining user experience. We have to be more intelligent in how we go through authentication, analysing behavioural patterns and using more data sources than the standard username-password combination."

Steve Bond, group head of cybersecurity at William Hill, adds: "We've got lots of good technical controls and there are lots of technologies out there, but if we want people to start adopting more secure behaviours and practices, we need to think about how we're asking them to do that. We need to ensure it's easy for them to do and that it fits with how they work. That is by far the biggest barrier to the adoption of better security practices and controls in William Hill. User experience is the most important aspect of everything we are doing."

> **Once you assume they're in, it changes the way you think about how to protect the business, and you end up protecting from the inside out rather than the outside in**

As well as mastering the balance between security and user experience in this new world of assumed breach, which relies on preparedness rather than prevention, CISOs must also act as a cultural change agent across the business. Departmental silos are a cybercriminal's best friend, so security leaders must transcend the entire organisation and playbook the scenarios for a real business recovery, not a security recovery, in the event of a cyber attack. The close alignment between the security and business strategy is absolutely fundamental.

"I often hear people ask: how are you going to build a security culture? But the question should be: how are you going to build more security into your business culture?" says Kevin Brown, managing director of security at BT. "The last 18 months has shone a spotlight on the role of the CISO as a business enabler – a transition, almost, from guard dog to guide dog. The business must recognise why security matters. It's now known that security is seen as a core business differentiator, as consumers want to know how you're looking after their data. An understanding of this across the business is key to building the right culture."

The technical recovery, in many instances, will actually be relatively straightforward following an attack. The business recovery is more of a challenge, and that's where it's critical that all of the people involved are working collaboratively, with strong alignment between the technology department, the security department and the rest of the business.

"When one team is left to deal with the recovery, they tend to divert their attention to what they know best, which, for a technology team, is the technical recovery," said Karl Hoods, CDIO at the Department for Business, Energy and Industrial Strategy. "Earlier this year I helped the Harris Federation, a group of 50 schools, with 40,000 students, recover from a ransomware attack and it required a whole organisational approach.

"Nowadays responsibility for security is much more integrated across organisations and it has to be that way or else you end up with a risk appetite and a set of controls which are misaligned. The days of the technical or security team working in isolation should be long gone"

Ultimately, the CISO must become a diplomat. Security is the glue that drips down between all the cracks of a business and joins all of the departments together. Businesses have seen the hugely damaging impact of supply chain attacks in the last year, and mustn't let their own departments fall to the same fate. That means permeating across the business to ensure security is thoroughly integrated, and utilising the latest in technologies like identity.

"Identity is where I see the next battlefield," says Craig McEwen, CISO at Anglo American. "You look at zero trust approaches and the other models of how people access what is now no longer a perimeter-based network – all of these ideas and future ideas are going to coalesce around identity. If you can get identity right, you can enable and facilitate future iterations of development in terms of how people work. Identity is where it ultimately lies."

For more information please visit cyberark.com

CYBERARK®

CIO ROLE

To succeed, today's CIOs must look outwards

To grasp the opportunities of the future, CIOs must look beyond their companies, placing customer needs at the heart of their efforts


Shannon Fagan via GettyImages

Emily Hill

"The doorway to success swings outwards, not inward," says author and spiritualist Robin S Sharma. Should CIOs pay attention?

That philosophical wisdom could certainly be seen in recent comments by Rashmi Kumar, HP senior vice-president and CIO. She argues that CIOs must stop focusing inward and look outside to thrive in an increasingly technological and digital world.

"Being CIOs, our purpose should be to put the customers first and not have technology drive decisions around how we implement that technology," the Senior VP and CIO suggested to CXOTalk's Michael Krigsman in September. "Don't try to solve a technology problem. Try to solve a customer problem."

That's a challenge even when you have the vast resources of HP. The global giant is evolving but relies on processes that have been in place for 30 years.

"It's not easy to take an 85-year-old company that has a very different mindset and our partners who are themselves busy in their own transformation, to pull them together to create that end-to-end, more efficient ecosystem" from a process and technology perspective, she says.

Kumar's advice – to concentrate on customer problems – delights Professor Simon Mosey, director of innovation and entrepreneurship at the University of Nottingham's Business School.

"Most companies have got innovation envy, so their chief information officer will constantly be hit over the head to ask: 'Why can't we be more like Amazon? Our customers expect delivery on demand, to be kept informed at all times and for every step in the process to be easy and convenient – if Amazon can do all that, why can't we?'"

Famously, all Amazon's innovations begin with a customer problem, Mosey notes. This means that "in a meeting of the high-ups, you have to set out on a page what problem a customer is having that you're going to solve or why your idea would improve on what they're doing already ... that entrepreneurial approach is baked into their decision-making at board level."

We tend to think of the CIO as an internally focused role, tasked with helping employees work in a slicker, more efficient manner, aided by IT. In the past, some CFOs perceived CIOs as spenders on IT infrastructures "that don't seem to impact the bottom line positively, a negative dent with not much to show for it unless you understand the frameworks being bought", says Lucy Kallin, managing director of the executive search agency Noventure.

> **Most companies have got innovation envy so their chief information officer will constantly be hit over the head to ask: 'Why can't we be more like Amazon?'**

This view has been revolutionised by the Covid-19 pandemic, Kallin says, when IT departments ensured their colleagues could work remotely. While most were seen as heroes, other companies thought "that's what they should do as standard," she adds.

Chief human resources officers (CHROs) and other board members are now faced with a workforce that's interested in hybrid working contracts. The market is more open than ever, enabling leaders to access skills beyond their geographical borders. In this context, "CIOs have to ensure that the solutions they implemented to solve a crisis have the legs to go the distance," Kallin warns.

Helena Nimmo is CIO at software company Endava. She thinks an increasingly outward-looking focus is a question of not just adapting to reality but embracing it.

"Technology has bled into every aspect of modern-day life and can have a hugely detrimental effect on a business's ability to function if it fails," she says.

Technology's crucial operational role means that more and more practical technologists are embedded in senior leadership teams, Nimmo adds, meaning "the value of technology to solve customer problems, not just internal ones, can be better realised. In my role as CIO, being a business leader – not just a tech leader – is essential to customer success."

> **The role should now be viewed as essential to customer success as it incorporates everything from operations to innovation to delivery, and most importantly, customer experience**

As Bill Gates has pointed out, "information technology and business are becoming inextricably interwoven. I don't think anybody can talk meaningfully about one without talking about the other."

Throughout the pandemic, organisations have scrambled to quickly create new digital properties, aiming to address business challenges like supply chain management, customer relationships and employee communications, Nimmo says. CIOs are now increasingly vital to ensure a competitive business edge and are responsible for a wider landscape.

"The role should now be viewed as essential to customer success as it incorporates everything from operations to innovation to delivery, and most importantly, customer experience – all at the same time."

It's increasingly hard to define what a conventional CIO does because the role no longer exists in the traditional sense. Nowadays the CIO's responsibilities depend on the sector and the size of the company. Technology is so pervasive and there are so many technology leaders and labels that it's difficult to draw a box around any C-suite role.

The board is an ever-expanding entity. Beginning with a CEO, companies soon

found they needed a CFO, then a COO and then a CHRO. Now it feels like new roles emerge on a daily basis. However, the businesses built for future success will always put the end user at the centre of their decision-making, as the giants of Silicon Valley have shown.

Ultimately, the CIO's approach will depend on their company's needs. They must develop a full understanding of the end-to-end processes that serve their customers. For example, Kumar is focused on changing printing needs and how HP can facilitate these to remain relevant in the future.

Data is now invaluable at a strategic business level, as well as internally. For many CIOs, leading, managing and implementing a digital transformation strategy is now a fundamental part of the role. This means employing talented people who can be trusted to deal with internal challenges, enabling CIOs to focus on external stakeholders. Delegation is all important when offering the best support to customers.

C-suites that fail to embrace diversity and inclusion can hold businesses back. The murder of George Floyd in the US in 2020 "catalysed a reckoning around racial injustice that led many corporate leaders to seek to evolve their organisations to meet today's tremendous societal challenges", noted the Harvard Business Review.

A survey of the publication's readers found that 65% of respondents did not think their organisations were diverse and inclusive. Its analysis showed that better diversity on the board improved decision-making.

Anyone in a position of authority – not just CIOs – should look at the business from the perspective of "others who are usually underserved or not involved in the innovation decision-making", says Mosey. A first step is to think of things from a customer's point of view, both in terms of existing customers and those the company is targeting.

"With tech groups particularly, they tend to neglect the customers that don't fit the profile of the senior management team, which is usually 'pale, male and stale'," Mosey argues. "So you're not looking at characteristics of gender, race or disadvantaged communities who aren't in a position of decision-making – they don't tend to be represented in innovation."

Companies need to gain insight into lived experience and develop systems and services to match. When the CIO thinks like an entrepreneur, they're able to adapt before their businesses are disrupted by nimbler startups. That's better than playing catch up or – even worse – finding they're too late to react and the business is doomed. This means harnessing the capabilities that the best CIOs have long cultivated.

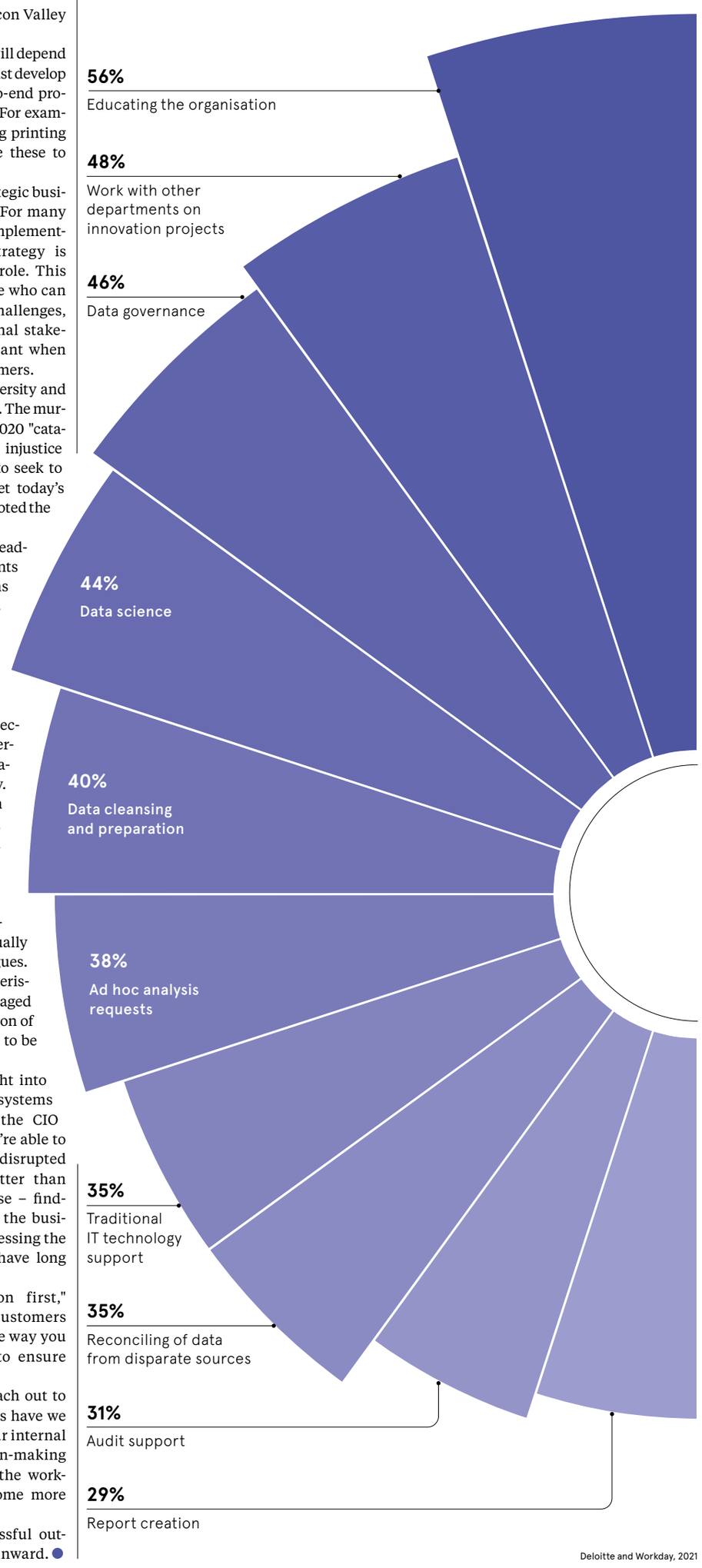
"Put the training wheels on first," Mosey says. Before asking customers about their problems, change the way you work within the organisation to ensure you can offer solutions.

The first step is actually to reach out to employees to ask: 'What problems have we got that we're not solving?'" If your internal systems, procedures and decision-making become more representative of the workforce, you should find you become more representative of customers.

Ultimately, the shift to successful outward thinking begins by looking inward. ●

WHAT THE CIO WANTS THEIR REMIT TO BE

Percentage of global progressive CIOs who say they would like to do significantly more of the following



Deloitte and Workday, 2021

Ezra Bailey via GettyImages

Does the C-suite still need a CTO?

At first glance, demands for a growing external CIO role might cause CTOs some consternation. Traditionally, their focus has been on external products, while CIOs focus on internal processes.

CTOs have concentrated on the customers, while CIOs look to employees. CTOs lead external innovation, while CIOs focus on internal productivity.

The distinction between CIO and CTO may seem opaque to outsiders. Essentially, CIOs focus on software, while CTOs look to hardware.

Cyril Silverman, CTO at DeepStream, sees the roles as two sides of the same coin. Both need to think about customer needs. "All information and technology decisions, whether internal or external, eventually impact the customer," he says, arguing that technology and information are distinct specialisms that require nuanced expertise.

Customers, workforce and technology choices are intertwined, Silverman says; ignoring this fact will lead to organisational systems that struggle to empower customers.

"In this fast-paced, digital era, there is an increasing premium attached to lateral thinking and creative solutions - the object is to cultivate a more entrepreneurial mindset because that, in a nutshell, is what being an entrepreneur is all about."

It's also worth remembering that historically, C-suite roles were filled by men. An Oliver Wyman report from last year suggested that as few as 20% of women hold these positions today. Among Fortune 1000 companies, the figures look even worse: women comprise just 6% of CEOs.

But with the future of companies so dependent on cutting-edge innovation, it's likely the CIOs and CTOs of the future will look very different.

"They will be more diverse - and not just demographically. More women and people of colour emerge as leaders in a sector that's mainly white male and middle aged. Remaining truly relevant is urgent for every CIO today," Kallin explains.

It's not just a case of working with stronger digital skills – the end client is different, Kallin notes.

"CFOs talk about growth and CIOs need to enable that, not just in terms of new toys from the CTOs but thinking – with that entrepreneurial mindset we need to cultivate – about what it all means for the customer experience and the ultimate success of the business."

But does a company really need both? For Mosey, the focus must be on the customer. That means C-suites need a chief innovation officer. He uses Apple as an example.

"Famously, they're very good at getting the hardware and the software right and actually on their board they have a designer. Getting the hardware (CTO) and software (CIO) to work together seamlessly would be my definition of what a chief innovation officer does."

Cyber resilience – planning for what happens after cyber criminals hit

Smart and determined threat actors are using ever more innovative means to attack your business, that's why cyber resilience – the ability to bounce back – is as in-demand as cybersecurity

As Graff jewellers count the cost of a hack exposing 69,000 client details, including those of Donald Trump and Oprah Winfrey, hacking groups are proving every week that they are capable of accessing any tier of business and society.

Ransomware attacks in particular have been taken to a new level of threat with 'ransomware as a service (RaaS),' pay-for-use tools which allow non-specialist criminals to become hackers. RaaS operations like the BlackMatter ransomware group even shut down farming co-ops in Iowa and Minnesota recently, impacting 2500 farmers.

As Lindy Cameron, CEO of the UK's NCSC (National Cyber Security Council), stated at the Cyber 2021 conference at Chatham House, "Many (businesses) have no incident response plans, or ever test their cyber defences."

The post-Covid, work-from-home workplace comprises hundreds, if not thousands, of devices, apps, data, and endpoints, all of which may be exploited by threat actors seeking to gain access and exploit data for profit. Cybercriminals hacked a US casino by accessing the Wi-Fi controlled thermometer gauge on an ornamental fish tank. They managed to steal a 10GB tranche of data.

This is why having a true disaster recovery solution is your best get-out-of-jail card against cybercrime, ensuring data can be recovered, no matter the situation.

The evolution of business continuity and disaster recovery (BCDR)

Backing up data alone is no longer enough, says Greg Jones, director of business development for the EMEA regions at Datto, a security and business continuity disaster recovery (BCDR) company which deals with the fallout from the increasing number of cognitive ransomware attacks.

"Once bad actors have compromised your network and have a copy of your data, they then go for your back up device and attempt to compromise or destroy it. That is exploding at the moment"

Because of this, cyber resiliency, unfortunately, is not a project you tick off by simply buying products. "Incidents will almost certainly happen, accidentally or maliciously," says Jones. "The focus for businesses should be on keeping systems up and running during recovery, to reduce downtime and minimise the overall impact of any cyber attack."

This is why air gap technology - a security mechanism previously only used by stock exchanges, banks and big government - has become a key weapon in the BDRC armoury as it seals off networks and data from any human or technological threats. Air gaps are an electronically disconnected network that cannot be accessed or deleted, allowing you to rely on these to redeploy your company in the wake of a cyber attack.

Businesses should seek to protect all data no matter whether it lives on laptops, desktops, physical servers, virtual servers or software as a service data, such as Google Workspace. "Follow the 321 rule," says Jones. "Keep at least three copies of your data stored. Two backup copies on different devices or storage media. Keep at least one backup copy offsite."

Creating a business that is cyber resilient

Cyber resilience addresses understanding the potential leaks and holes in your business processes - whether they are human or digital - and seeks to have a plan in place focused on three key pillars: people, processes and technology. Datto advises businesses about the weak links caused by people and processes first and only when these have been covered do they then fill in any gaps with technology.

These weaknesses in business processes are often not obvious from within the company. Hackers can target casual or permanent staff with bribes to provide access and there are even weaknesses when hosting in-person events. Vertical-specific events, such as banking conferences, have been targeted with hackers taking promotional USB devices from marketing stalls at the event.

> **When looking for a business continuity and disaster recovery solution, businesses must ask the question: how long can they afford to be offline?**

"They'll keep the promotional people talking while a second person takes a handful of the drives away, goes to a cafeteria and loads malicious software on there. They then return to the stall and drop all the devices back into the jar, potentially infecting however many banking organisations." says Jones.

It is also key to reduce the level of access staff have, not just for deliberate misuse but for accidental damage.

"Approach everything with zero trust," says Jones. "The CEO should actually have almost the least access within the business from an IT point of view. Why give them the keys to the kingdom - i.e. an administrator's account? In many instances people are given way more than they need - apply the theory of minimal access control."

To create a multi-layered approach, apply single sign-on and two-factor authentication controls as well as cloud deletion defences. This reduces the impact of any accidental or malicious attacks.

How long can you afford to be offline?

When looking for a business continuity and disaster recovery solution, businesses must ask the question: how long can they afford to be offline? If it's any period longer than a few minutes, businesses have to plan ahead to mitigate risk.

Business recovery should create a recovery point objective (RPO), which details the amount of data that - after your most recent backup - your operation can lose before significant harm occurs. From there, create a recovery time objective (RTO), which understands the amount of time that a system or application can be down without causing significant damage to the business, as well as the time spent restoring the application and its data.

This helps you understand the size of the window of opportunity your business has to bounce back from a cyber crisis. A true BCDR solution should have you up and running in minutes, not hours, days, or weeks and it should take into account all disaster risks.

This can mean, if you are using an off-site data storage solution, that your data centres are in a secure location. "At Datto we have twelve data centres around the world," says Jones. "We take hundreds of checklists into consideration before we decide on a location. For example, the location must not be on a flight path, a floodplain, or be an earthquake risk."

In an era of supply chain shortages, businesses looking to buy new servers can sometimes face significant lead times with regards to delivery, in some cases weeks or months for delivery. However, smart BCDR should also negate this risk. "We can have you operational within minutes, no matter what the issue is" says Jones.

The question facing many businesses is not if they might face a cyber attack, but what they will do if and when one is successful. It is sensible to have a parachute in place, and that includes BCDR expertise in creating a holistic 360 degree approach to protecting your business in the digital age.

For more information please visit datto.com

datto

SMES

How to hire your first CIO

It's the first time your business has recruited a CIO. How do you ensure you find the right person for the job?

Sally Whittle

As technology grows in importance for a range of businesses, many will consider hiring a CIO. So what does the recruitment process involve and what skills should you seek in the winning candidate?

Businesses now face huge demand for secure hybrid working and integration of multiple cloud-based apps and services, not to mention the need to incorporate digital transformation into the broader business strategy. Isn't it time someone took charge, ensuring your technology strategy and business strategy are fully aligned?

If you're at the point in your business journey where you know that technology will play a central role in driving growth and shareholder value, you're probably ready for your first CIO, says Anna Barsby, co-founder of consulting firm Tessiant and former CIO at Asda, Morrisons and Halfords.

"Adding a CIO to the management team helps to drive growth because it improves your IT strategy and efficiency. Making processes more efficient reduces costs and frees up employees to focus on higher-value tasks, which in turn drives more value," says Barsby.

Despite the widespread skills shortage, there's a good chance you'll be inundated with applications for a new CIO role, says Joe Topinka, a chief information security officer (CISO) with Fortalice who provides consulting and coaching to new CIOs.

"Recently, the HR director at a mid-sized company told me they'd received 300 applicants within 24 hours of posting a vacancy for a CIO on LinkedIn," says Topinka. "There is great value in finding an experienced recruitment search team who have 'been there and done that' before," he says.

Barsby also recommends using specialist support to identify the right candidate. "I've seen people just hire someone they know already who knows about IT, and it generally doesn't work too well," she says.

That's because a successful CIO must be a conduit between your business leadership team and the IT team. They need to understand how to leverage technology to deliver against a business strategy, as well as identifying opportunities to use technology to improve business efficiency, performance and innovation.

Your CIO will need to know about more than just technology. "The CIO role has changed enormously over the last decade and the new breed of CIO is definitely people first, technology second. Modern CIOs need to understand that technology is an enabler of people," says Barsby.

Working with a specialist recruiter can help you identify candidates who combine the technical expertise required of a CIO with the necessary communication and strategic skills. The CIO job description needs to prioritise business strategy over technology, while also stressing the importance of being able to lead and inspire people to embrace change, says Chris Underwood, managing director of executive search firm Adastrum Consulting.

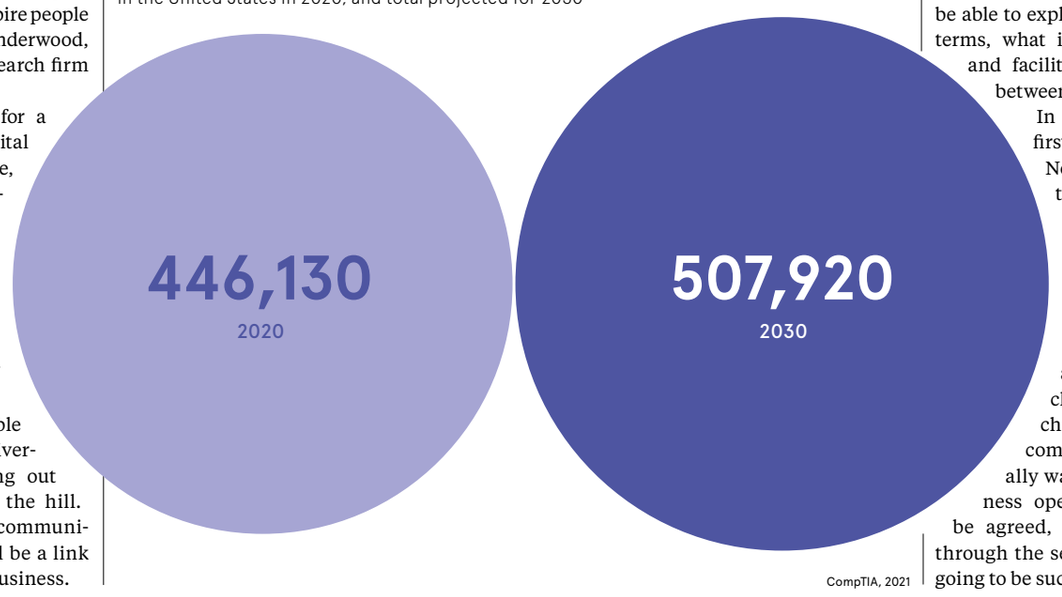
Underwood suggests looking for a CIO with high levels of both digital and emotional intelligence. "To me, digital intelligence is understanding digital innovation and how to exploit it to deliver against business objectives, while emotional intelligence means someone can unite teams to embrace change, which helps you to retain the best talent and develop future leaders," says Underwood.

An effective CIO needs to be able to lead and inspire people, delivering change while also watching out for future change coming over the hill. Above all, they must be a good communicator, adds Barsby. Your CIO will be a link between the tech world and the business.

sinology via GettyImages

DEMAND FOR CIOS SET TO RISE

Total number of chief information officer and IT manager jobs in the United States in 2020, and total projected for 2030



CompTIA, 2021

"They need to be an interpreter in some ways, understanding what the business needs and conveying that to technology professionals," Barsby says. "Equally, they must be able to explain to the board, in business terms, what is possible with technology, and facilitate a two-way conversation between business and IT."

In some respects, hiring your first CIO might be the easy part. Now you need to be ready for the changes that their role will bring. Many business leaders employ a CIO to deliver change but then struggle to adopt that change themselves, says Underwood.

"It is very easy to talk about transformation and change, but it can be really challenging when someone comes into a CIO role and actually wants to change how the business operates. That change has to be agreed, accepted and cascaded all through the senior leadership team if it is going to be successful," he says.

Top questions for a potential CIO

01 What's your track record?
Your CIO should have a legacy of delivering business strategy. Ask about how they have achieved and evolved strategy in previous positions – this is more important than specific industry or platform experience.

02 Can you add value?
Along with being a business leader, your new CIO needs to have the experience to focus on projects that drive revenues or profit. Do they understand how their current project portfolio performs in these terms?

03 Are you an effective talent coach?
Executives are often afraid of technology, so look for someone you wouldn't be scared to ask a dumb question. Ask about prior experience coaching a team – do they help build skills and knowledge in their wider team?

04 Are you a partner?
A great CIO doesn't just deliver technological services. They should be a strategic partner, happy to take an active role in driving strategy. They must collaborate with other business unit leaders and use technology to drive strategic growth.

CIO or CTO: what's the difference?

For many years the terms CIO (chief information officer) and CTO (chief technology officer) were used interchangeably. However, that's no longer the case.

Today, a CIO is a business strategist who advises the leadership team on how to leverage technology to deliver business innovation, transformation and strategy. A good CIO understands IT systems and services, but they don't need to be an expert in specific platforms or technologies. Their role is to understand how technology helps the organisation deliver its strategy and become more efficient.

Meanwhile, the CTO is someone who handles the operational side of IT, helping to shape how IT platforms and applications need to evolve to meet the organisation's strategic needs. A good CTO is a technical visionary, with a strong understanding of new technology services and platforms. They will often be responsible for liaising with external suppliers and partners to build an effective IT architecture.