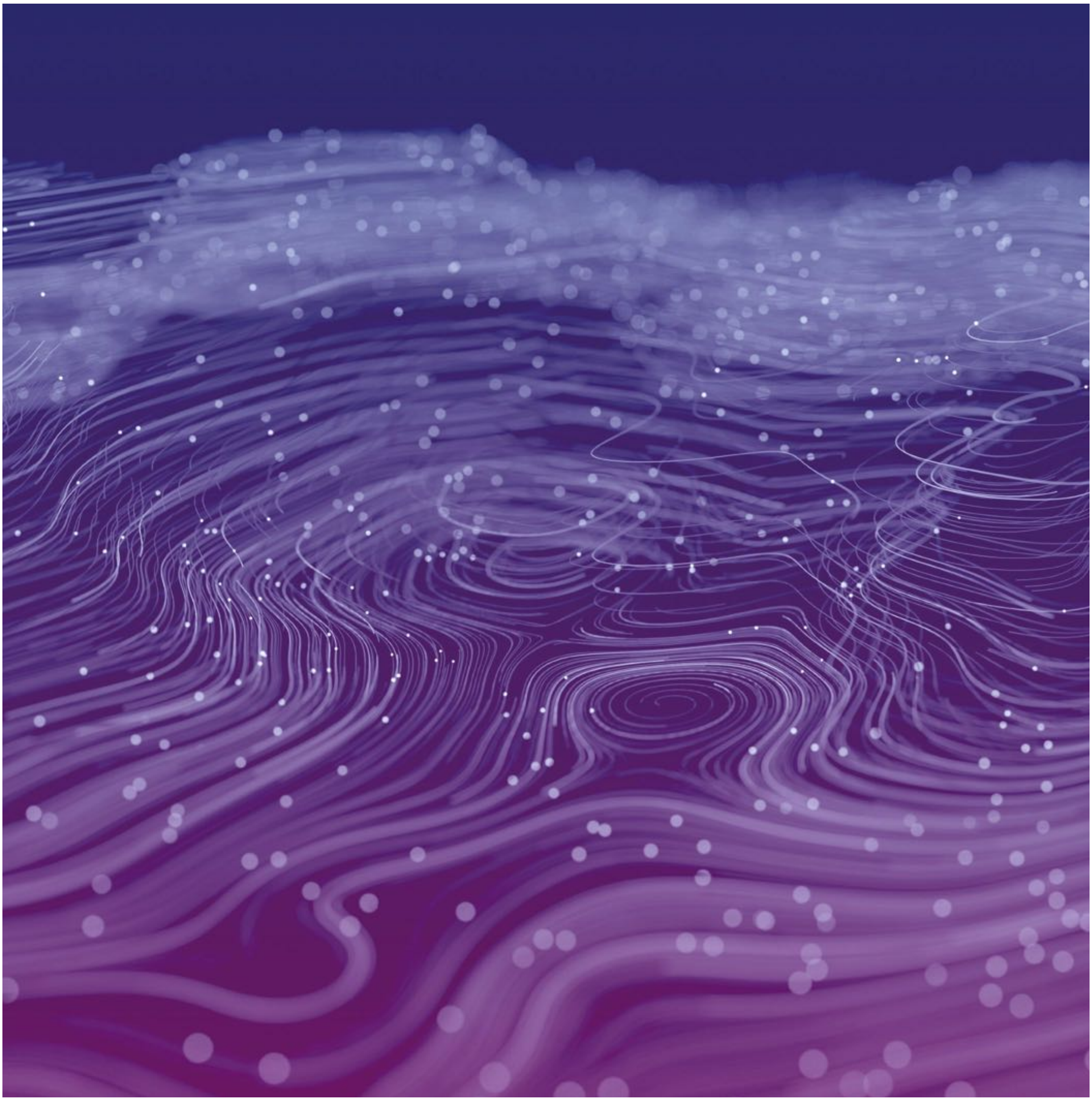


CYBER SECURITY IN THE AGE OF DIGITAL TRANSFORMATION

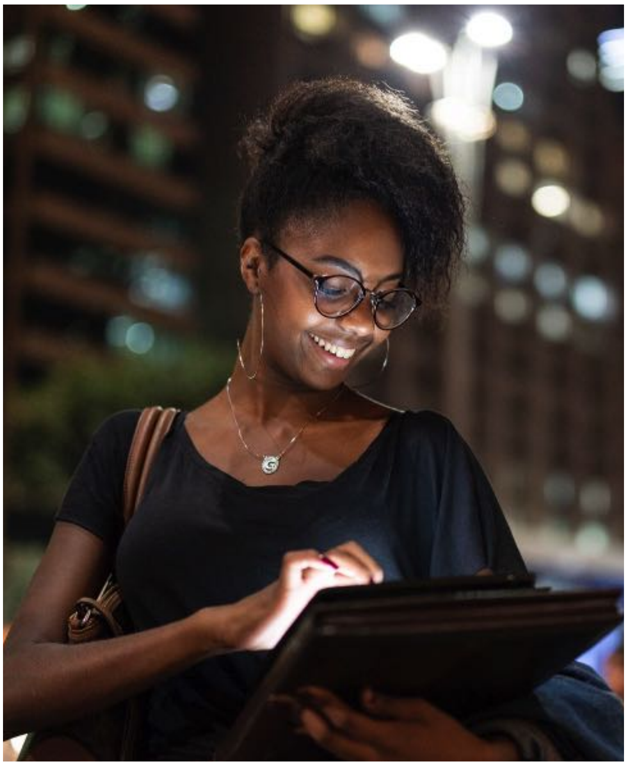
A reality check

NOMINET
CYBER
SECURITY

DIGITAL TRANSFORMATION: WHERE OPPORTUNITY MEETS THREAT

It's no secret that digital technology has transformed the way we do business. It's also no secret that many more changes lie ahead. Almost every year, a new digital technology arrives that disrupts the status quo and opens new operational vistas for enterprises. From the cloud, mobile and social innovations that have already changed our world, new advances in virtual reality (VR), blockchain, AI and quantum computing will arise and continue to reshape how we work and live.

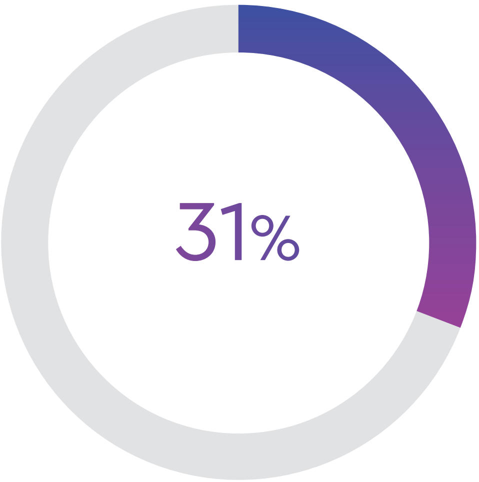
Today, many enterprises are already digital to the core. Those that aren't soon will be. So ubiquitous is digital technology in enterprises, that some commentators think the initial process of digital transformation is nearing fulfilment. For Accenture, digital is now just the accepted way of operating. It believes we are entering a 'post-digital' era where businesses will need to innovate further and faster, and deliver against individual customer demand in real time.[1]



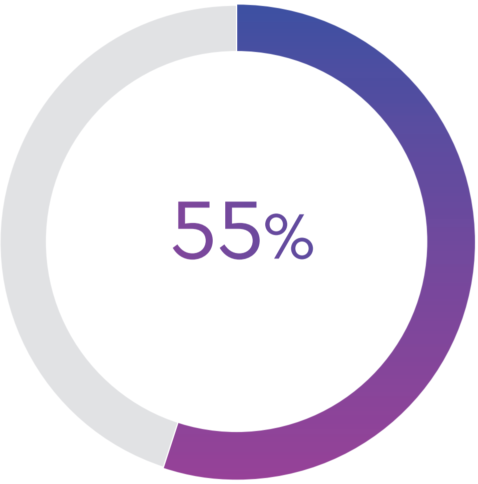
The world that is emerging is therefore one of new opportunities. However, the digital transformation of industry and enterprises also brings with it major challenges. One of the most pressing is security. As our world becomes increasingly connected and technology more sophisticated, the threat landscape becomes more complex and potentially damaging. A greater exposure to digital technology means a greater exposure to system vulnerabilities, 'as the tools being used by businesses to innovate, like AI and machine learning, could be vulnerable to attack and are also being used by hackers.

We wanted to dig deeper into the key intersection of digital transformation and cyber security through the lenses of those tasked with protecting their enterprises, such as Chief Information Security Officers (CISOs), Chief Technology Officers (CTOs) and Chief Information Officers (CIOs). We have carried out research to collect and analyse a large enough dataset to give valid insights into the opinions, behaviours and mindsets of cyber security leads at large enterprises in the US and the UK.

[1] Accenture



31% of senior security professionals report 11–25% of digital transformation budgets are allocated to security, but…



55% of senior security professionals say customers and partners query the robustness of their security stack

Our findings provide a reality check on digital transformation by outlining where organisations actually are in the process, why they are transforming and how this impacts their cyber security posture. The data provides three key insights:

1 Digital transformation is predominantly an IT-led initiative within enterprises, with more education needed for board level decision makers to support transformation initiatives.

2 Cyber security should be considered at the earliest possible stages of digital transformation initiatives. Where this has not happened, remedial action should be taken fast.

3 Security teams should seek advice from a broad range of vendors and analysts to ensure a comprehensive security solution.

THE 'WHY', 'WHO' AND 'HOW' OF DIGITAL TRANSFORMATION

If there was any doubt lingering that the future lies in the wholesale transformation of the enterprise through digital technologies and business models, our survey shows it is misplaced.

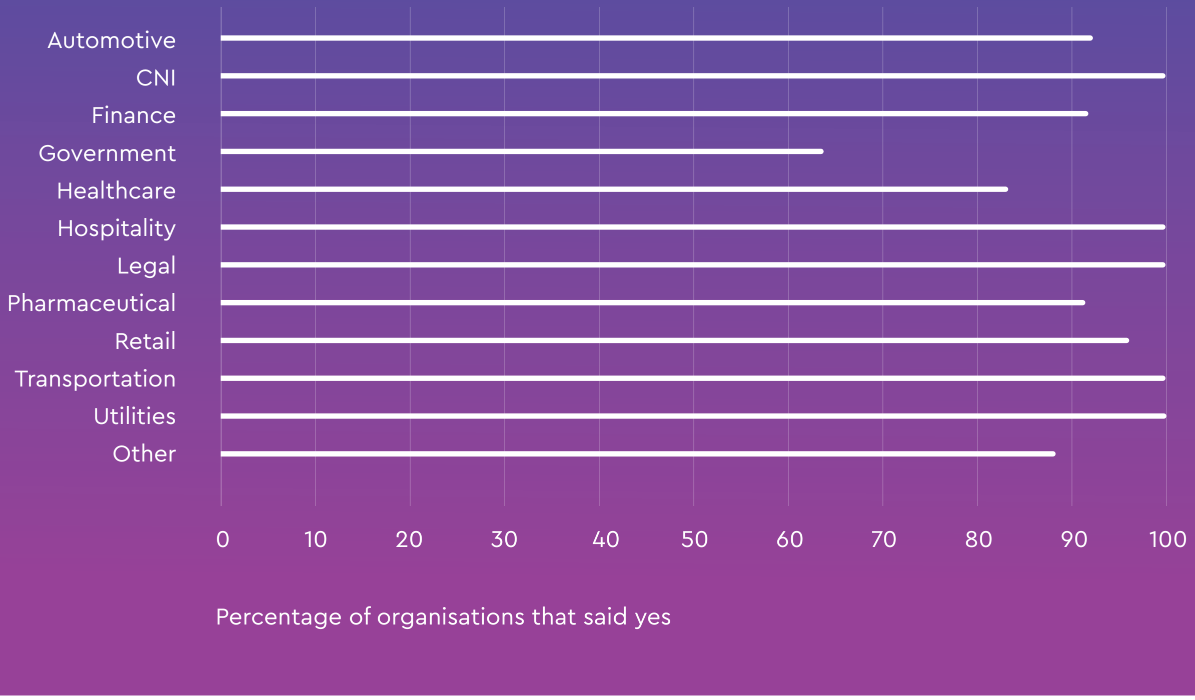
The vast majority (93%) of the people we interviewed said that their organisation was either currently engaged in, or planning to engage in, a digital transformation programme. This appetite for digital transformation spans all industries and sectors. Even the in the most cautious of sectors, government and healthcare, there is still a strong majority reporting a move towards digital transformation (67% and 86%, respectively).

Roadblocks to digital transformation

Before we look at what's driving this powerful trend, it's worth considering the small proportion of respondents who claim not to be considering digital transformation projects in their firms. While only a small minority of organisations: 4% in the UK and 6% in the US, it is still a significant finding and strongly begs the question: 'why not'? Surely these firms are putting themselves at a huge and unnecessary competitive disadvantage?

Our data suggests that the leadership in these firms may in part be the cause. Although 5.5% of respondents represents a small proportion of the set, nearly half of them (47%) said that a lack of vision in their company was to blame. Others cited resistance to change (40%) and legal, risk management and compliance concerns (40% - a particular concern for respondents from heavily regulated industries like financial services, government and healthcare).

IS YOUR ORGANISATION CURRENTLY ENGAGED, OR PLANNING TO ENGAGE, IN A DIGITAL TRANSFORMATION PROGRAMME?



A further 28% said it was because the cost of digital transformation is too high and 27% because they were concerned about the increased cyber security risk.

Clearly, digital transformation brings with it a fair degree of risk. But all risk, whether operational, regulatory or cyber security-related, must be weighed against the greater risk of doing nothing and falling behind in the market.

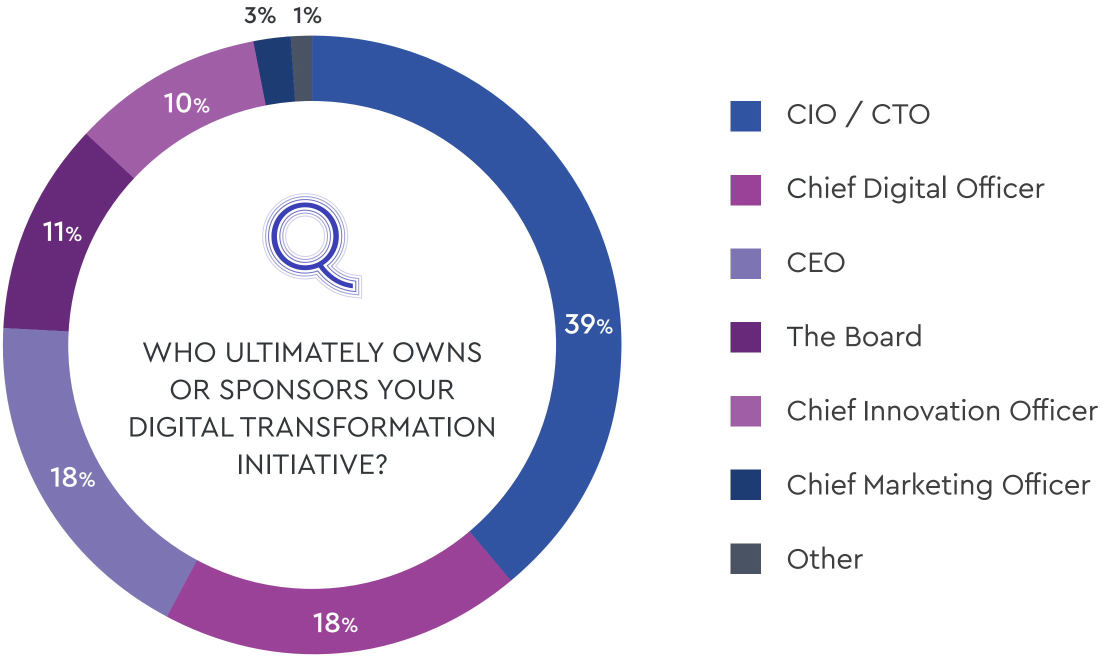
The IT team in general and security professionals in particular can help business stakeholders make this case by demonstrating how cyber risk can be managed, even as the enterprise opens up to the digital world.

Who owns digital transformation in organisations?

Returning to businesses that are embracing digital transformation, and stopping to consider their motivations and drivers, let's look at which business leaders 'own' or sponsor transformation initiatives.

What's immediately clear is that in most firms, IT is still the ultimate owner of digital transformation. According to 39% of the people we polled, the CIO or CTO is the main business sponsor of their transformation initiatives, well ahead of other functions – including the Chief Digital Officer (18%) and Chief Innovation Officer (10%).

Given the ongoing debate around whether firms need to employ a Chief Digital Officer to drive digital transformation, these are interesting findings.[2] They suggest one of two things. Either digital transformation is still largely led from a technical rather than a business perspective, or (in Nominet's experience, most likely) CIOs/CTOs have transformed themselves, and are now offering the mix of business and technical leadership needed to make digital transformation a success.



[2] The Leadership Network

Building a transformation team

Digital transformation is an enterprise-wide initiative and it requires a team with significant resources and focus. How are organisations approaching this requirement? According to our panel, and as you might expect given that the CIO/CTO is usually leading transformation initiatives in the firms surveyed, the digital transformation team is nearly always a sub-set of the larger IT organisation (selected as such by 84% of respondents).

However, a significant minority (16%) report that their digital transformation teams are separate from IT. This trend was twice as likely in the US than in the UK (20% vs. 10%), perhaps suggesting a variance in corporate culture.

From a security perspective, having the digital transformation team under the umbrella of the IT organisation appears to be the best approach. When asked to rate the effectiveness of their security stack on a sliding scale of one to ten (with ten being the most effective), respondents from organisations where the transformation team is integrated with IT were much more likely to score themselves between seven and ten than those with a separate transformation team (86% vs. 14%).

Similarly, when it comes to their organisation's overall security posture, companies that integrate IT and digital transformation teams are much more likely to be very confident than those with separate transformation teams (85% vs. 14%).

Our survey is of people from roles within the traditional IT team. These findings could therefore suggest selection bias, but they could just as likely speak to a lack of transparency into the work of digital transformation teams that are not incorporated with IT. Regardless, where firms are running transformation initiatives, it is vital that the wider security team can review the transformation at hand as part of a complete organisational security posture.

To outsource or not outsource?

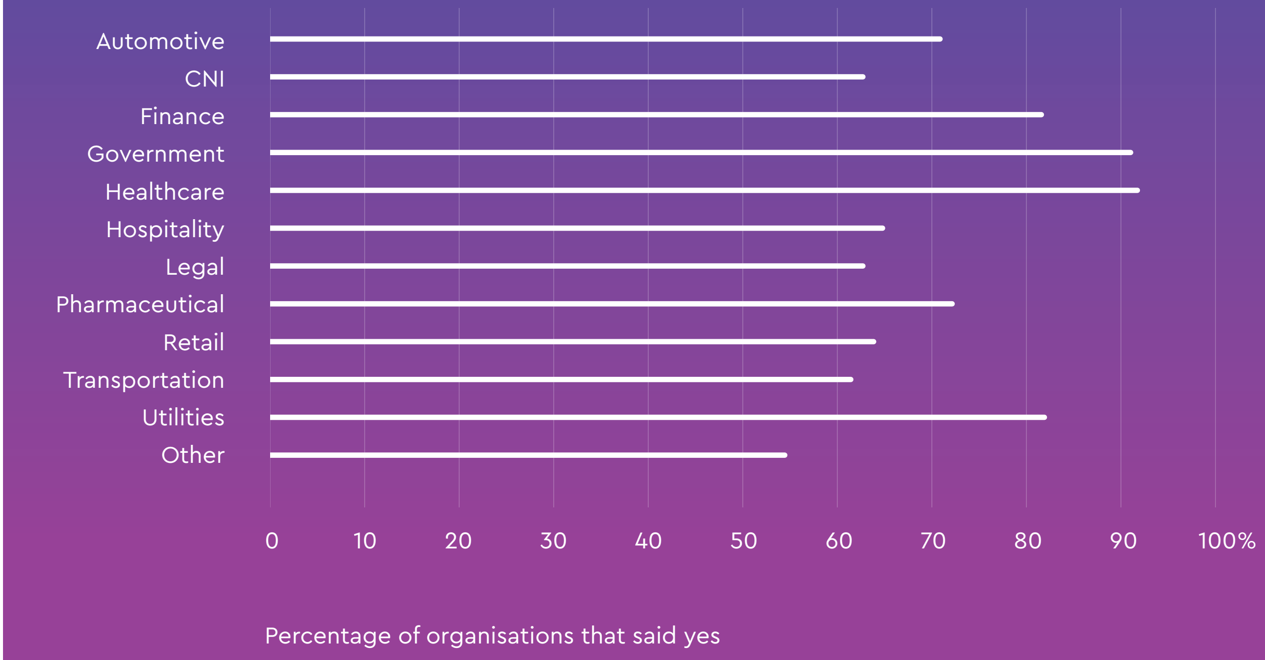
Another factor relating to the 'how' of digital transformation is whether organisations feel comfortable in using outsourced service providers to help them complete their initiatives. In a large part thanks to cloud computing, outsourcing has the potential to accelerate digital transformations while moving costs from a CAPEX to an OPEX model. Such services underpin many of the enterprise innovations that are increasingly considered key to digital transformation, such as Agile and DevOps.

Outsourcers also, of course, enable access to next-generation security capabilities. In fact, security is as much a product of digital transformation as it is an enabler. Accessing security services from cloud-based providers allows firms to leverage the very latest in security innovation rapidly and cost-effectively.

Security professionals we interviewed reported that their businesses are aware of the opportunities on offer with outsourcing: 72% say that their organisation already outsources elements of their transformations. This proportion was higher in the US than the UK (75% vs. 68%), again likely reflecting slight differences in the maturity and cultures of the markets.

Interestingly, firms in sectors such as finance (82%) and government (93%), which have traditionally been more cautious of outsourcing due to regulatory pressures, now appear to be embracing the opportunities on offer. This may reflect the maturity of the outsourcing market and the fact that the outsourcers themselves often deliver the highest levels of digital security.

DO YOU OUTSOURCE ANY OF YOUR DIGITAL TRANSFORMATION PROGRAMMES?



The drivers of digital transformation

Returning to our original question: why is digital transformation such an overwhelming trend? As a key topic of interest, our survey provides an interesting take on the matter from the security perspective.

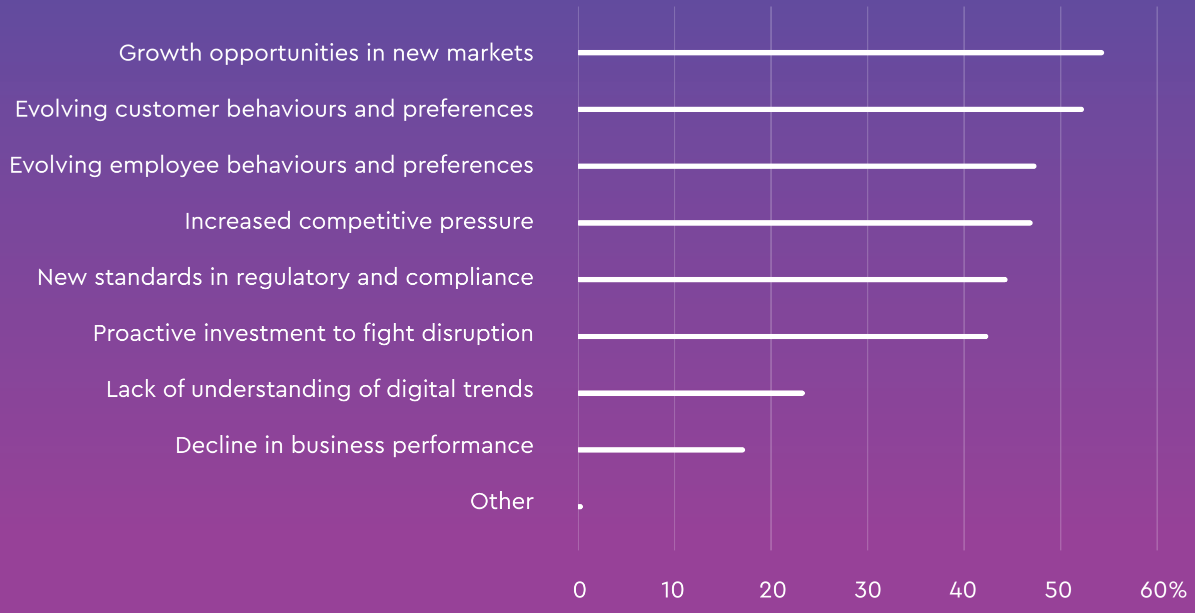
As might be expected, the core drivers relate to the age-old business desire for growth and the more recent requirement to meet the demands of today's digitally literate customers, who tend to demand much more of the companies they use.

These numbers chart a well-understood dynamic where firms can only secure customer and employee loyalty by using the latest digital technologies. The resulting experiences drive customer loyalty, attract and retain top talent, and ultimately enable growth.

These drivers are reflected in the digital transformation priorities of businesses. We asked our respondents to rank various priorities in order of importance. Way out front was IT and customer service, selected as a first, second or third choice priority by 72% of respondents – 41% listed it as their number one priority. This was well ahead of other areas such as innovation and operations, which were selected as top-three priorities by 40% and 37% of respondents respectively.

These findings were broadly similar across industries, with the exception of government. Security professionals at these organisations were more likely to select innovation as a key priority for their digital transformation initiatives (29%).

WHAT ARE THE KEY DRIVERS OF DIGITAL TRANSFORMATION WITHIN YOUR COMPANY?



The state of play

In the opinion of those we interviewed, businesses have clear digital transformation goals and are steadfast in their wish to implement them. But how far have they got?

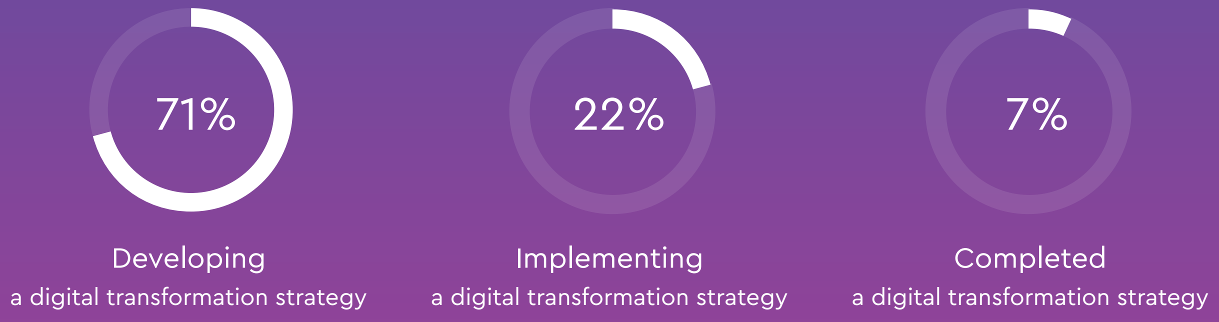
Only 6% report having completed their digital transformation. While the organisations our respondents work for have undoubtedly completed significant elements of digital transformation by, for example, implementing Software-as-a-Service applications or joining up their data across back and front offices, there is a question to be asked about whether digital transformation can ever really be complete. In Nominet's view it is an ongoing process that will continue over time as business requirements change and technology evolves.

This small proportion of very confident respondents aside, the majority say that their business is either still developing its digital transformation strategy (40%) or implementing a strategy (34%). Others have developed a strategy but are not yet in the implementation phase (21%). US firms seem to be slightly further ahead of their UK counterparts in this respect, with 39% in the process of implementing their strategies, compared to 28% in the UK.

Significantly, there seems to be a correlation between cyber security events and progress towards implementing digital transformation strategies. Where our respondents have reported a cyber attack within the past 12 months, they are half as less likely to be implementing their transformation strategies as those that have avoided security incidents (22% vs. 42%). Although it's impossible to know if this is a causal relationship, it is interesting to note that the likelihood of a business implementing a digital transformation strategy decreases as the number of security breaches increases.

WHAT IS THE STATUS OF YOUR DIGITAL TRANSFORMATION PLANS?
HAS YOUR ORGANISATION EXPERIENCED A CYBER ATTACK AND/OR BREACH WITHIN THE PAST 12 MONTHS?

Percentage of respondents with security breaches in past 12 months



The cost of digital transformation

How much are businesses willing to spend on their digital transformation initiatives? According to the security professionals we spoke to, budgets in a single year can span a few million dollars/pounds all the way up to over £/$1bn (3% in the UK and 4% in the US). Budgets will of course vary according to the size of the organisation, but some of the variance in our survey might reflect differences in the level of commitment to digital transformation strategies and whether this encompasses discreet projects or company-wide initiatives.

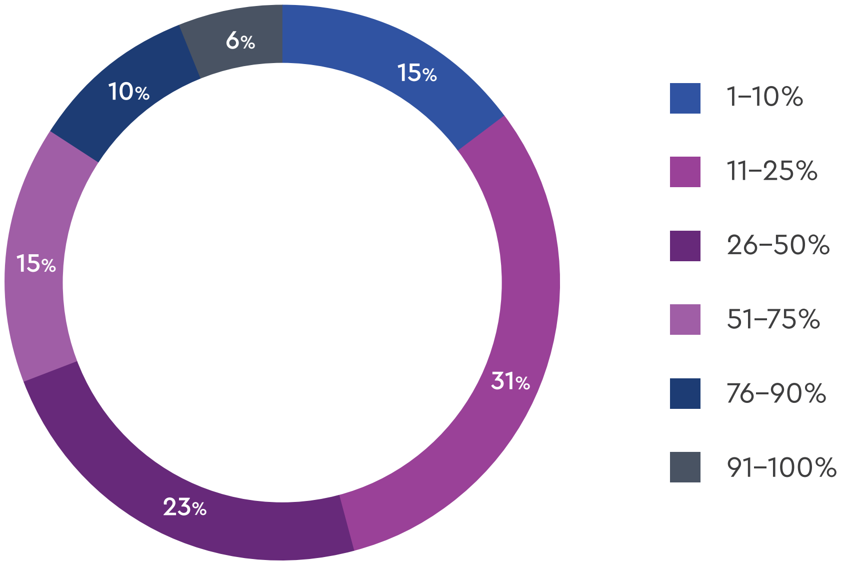
On average, however, organisations in the UK are most likely to spend between £50m and £100m (14%) in a financial year. In the US, businesses are most likely to spend between $50m and $100m (13%), although a significant proportion spend between $250m and $500m (12%).

In relative terms, this spend is still just a fraction of total IT budgets. For 31% of organisations, digital transformation accounts for 26–50% of IT budgets. This may seem like a large number, but given the scale of enterprise-wide transformation required by many firms, it may not be enough.

That's why it's encouraging to see that 19% of the people we spoke to said 51–75% of their IT budgets are being spent on digital transformation. A subset of 'super transformers' claim that 76–100% of their IT budgets are going to their transformation initiatives (14%). Arguably these firms are putting themselves in the best possible position for the future.

Of course, of most interest to security teams is how much of this budget is going towards cyber security. At most organisations, respondents reported that figure to be around 11–25% of IT budgets. This is, of course, either very good or very bad, depending on the size of the total pot.

APPROXIMATELY WHAT PERCENTAGE OF YOUR ORGANISATION'S TOTAL DIGITAL TRANSFORMATION BUDGET GOES TOWARDS CYBER SECURITY?



Interestingly, 6% of respondents said that 91–100% of their transformation is going to cyber security budgets. Perhaps these organisations are using security as a starting point for their transformation: putting in place the most advanced levels of security before moving on to wider business transformation – an approach that is not without its benefits.

Overall, the proportion of digital transformation budget that firms are willing to spend on cyber security increases in line with the number of attacks directed at the business. For example, 53% of respondents at organisations that have been targeted more than 30 times in a year by cyber criminals report that 76–100% of their budget now goes on cyber security. Perhaps these numbers reflect a small cohort of firms that have been attacked extensively and are turning to digital transformation as a way of increasing their enterprise security.

A cause for concern

Of course, any major enterprise transformation comes with its fair share of risk, and digital transformation is no exception. Cyber security is far and away the biggest cause for concern from the perspective of the people we spoke to.

When asked to prioritise their top concerns, 53% of respondents listed cyber security as a top-three threat. This compares to other worries such as budget (41%) and having a rigid technology infrastructure (40%).

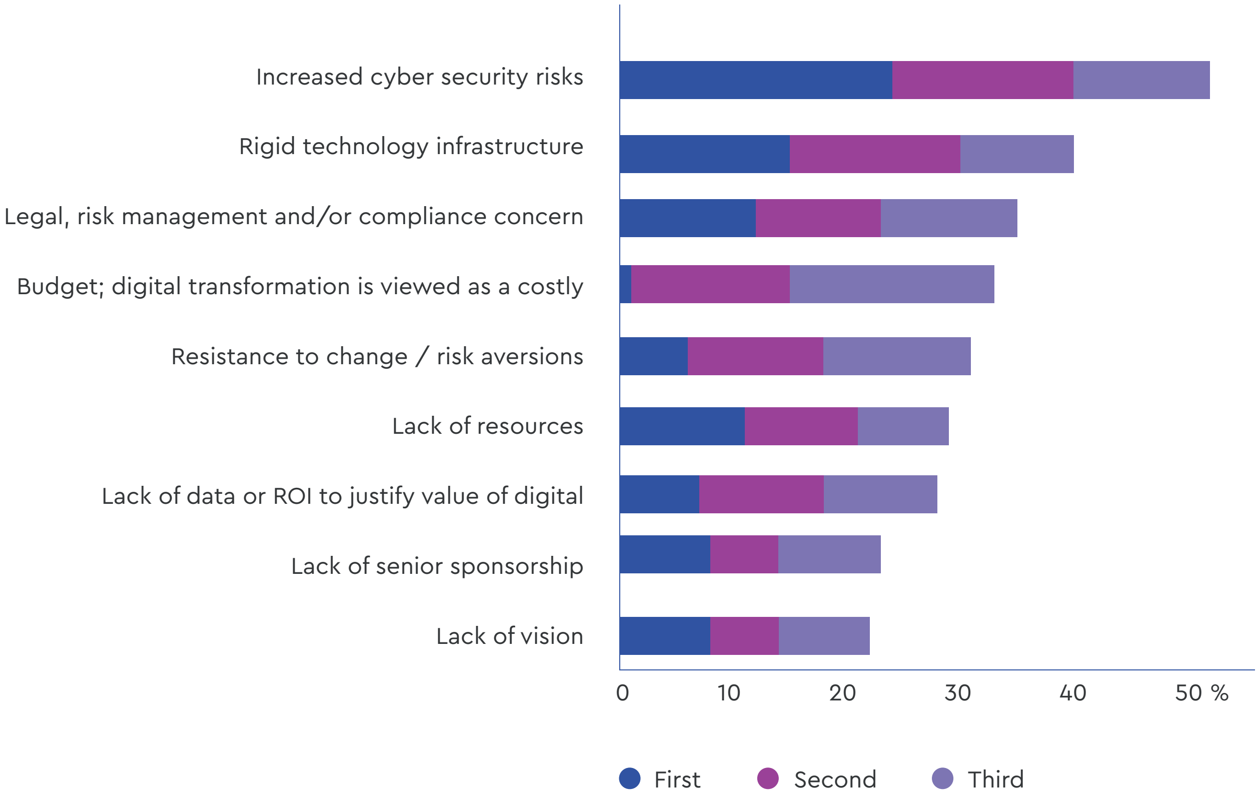
So, well ahead of having enough money to fund transformation, to having senior sponsorship or even legal and compliance concerns, cyber security is seen as the single biggest risk when it comes to digital transformation. In fact, the vast majority of the people we spoke to (95%) expressed some level of concern around cyber threats – 41% were either 'very' or 'extremely' concerned. The level of concern was highest in the healthcare sector (two-thirds said they were 'very' or 'extremely' concerned) and the pharmaceuticals sector (57%), which is unsurprising given the sensitivity of the data these providers handle.

When asked to provide detail about the types of threat that are providing most concern, respondents noted a broad array of threats in reference to digital transformation. The one area slightly ahead of the others, exposure of customer data (60%), is perhaps front-of-mind given the recent focus on GDPR and the considerable fines that come with any instances of data theft at an organisation.

Perhaps of most concern is that not all businesses are looking to mitigate these threats at the earliest stages of their transformation projects.

While around a third of the security professionals we spoke to reported that, as we would hope, cyber security was considered during the development of their organisation's digital transformation strategy (34%), there were many that reported their businesses were leaving it to either the pre-implementation stage (28%), the implementation stage (27%) or even post-implementation of the digital transformation strategy (9%). Of concern, 2% reported that cyber security wasn't considered at all.

PLEASE RANK THE FOLLOWING IN ORDER OF CONCERN WHEN IT COMES TO YOUR ORGANISATION'S DIGITAL TRANSFORMATION EFFORTS



With 82% of the people we spoke to saying that cyber security was considered early enough in their digital transformation initiatives, it is possible there is something of a perception gap here. Significantly, 85% of this same cohort scored their security stack the highest effectiveness ranking of between seven and ten. All this despite the fact that 86% of them had experienced a breach in the past 12 months.

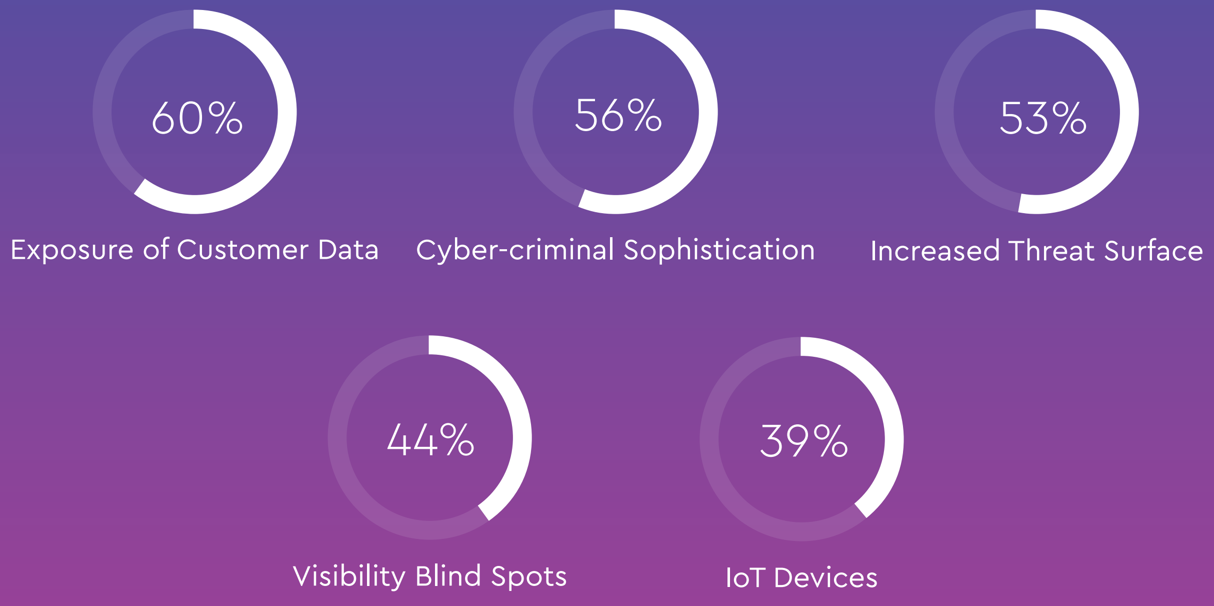
It is also worth noting that many report that important stakeholders have queried the robustness of their security stacks – including partners (59%), customers (55%) and industry/regulatory bodies (54%). From Nominet's perspective, it is best practice to consider cyber defences from the very outset of a digital transformation programme.

However, for businesses that have started their transformation programmes without considering cyber security, it is never too late to start. The market provides a wide range of security solutions that can be built into existing systems to provide a wrap-around security approach.

Indeed, the professionals we spoke to said they are seeking outside advice to help enhance their security posture. In fact, most of the professionals who participated in our study reported seeking advice before buying a security solution – and from a wide variety of sources including vendors (53%), consultancies (53%), analysts (52%) and outsourced cyber security providers (40%).

This is exactly the right course of action to take. One of the benefits of digital transformation is that it helps firms connect, engage and collaborate more easily with external partners. This ability should be leveraged to build strong security partnerships that add more value to in-house teams, bring greater capabilities than expertise and help create a more secure environment that could be achieved by a company working alone.

WHAT ARE YOUR CONCERNS?



SECURING THE FUTURE: DIGITAL TRANSFORMATION HAS ALREADY CHANGED THE WORLD

For consumers, digital transformation has reshaped everything from how we bank and get around town going on holiday and shopping for goods. For businesses it has enabled new back-office efficiencies and created ecosystem partnership models where businesses interact on a new scale and provide new types of personalised and subscription-based services. For citizens, it has helped transform the way public sector and healthcare services are delivered, improving access while driving down costs.

This is just the beginning. As advances in AI and machine learning, blockchain, quantum computing VR and other emerging innovations take root, our world will continue to change at an increasing rate. The new services, business models and industries that will emerge from our era of continual innovation can only be estimated today, but one thing can't be taken for granted: effective cyber security will be central to their uptake and success.

This is because digital transformation is built on the foundation of trust. Without it, consumers will steer clear and businesses will retreat into more secure and less risky alternatives.

There's little wonder therefore, that our snapshot of opinions reflects optimism and derring-do around the opportunities of digital disruption, but also caution about the threats that may emerge and what these might mean for the business.

Overcoming these threats will not be easy. It will require strategic thinking about security throughout digital transformation projects, so that the key questions asked at the strategy stage are not just 'will this project drive revenue or efficiency' but also, 'will it be secure and will it increase trust in our business?'

Fortunately, this is not something organisations need to do alone. Thanks to a thriving outsourcing, market and developments in security technologies, APIs and cloud platforms, firms can work with security partners to bring in expert, independent advice as well as the capabilities they need to address a dynamic security environment flexibly and effectively.

There is much to play for. Digital transformation has made, and will continue to make, household names of new companies and agile disruptors. But the rewards will only go to those companies that have thought seriously about their security posture and taken the appropriate measures.

METHODOLOGY AND EXECUTIVE ANALYSIS

Nominet commissioned a survey of 274 Chief Information Security Officers (CISOs), Chief Technology Officers (CTOs), Chief Information Officers (CIOs) and other professionals with responsibility for overseeing the cyber security of their organisation.

Respondents were sourced from large organisations (with 2,500 employees or more) within the UK (117) and the US (157), spanning a range of industries and sectors including automotive, Critical National Infrastructure (CNI), finance, government, healthcare, hospitality, legal, life sciences, retail, transport and utilities.

ABOUT NOMINET

Nominet is driven by a commitment to use technology to improve connectivity, security and inclusivity online. For more than 20 years, Nominet has run the .UK internet infrastructure, developing an expertise in the Domain Name System (DNS) that now underpins sophisticated threat monitoring, detection, prevention, and analytics that is used by governments and enterprises to mitigate cyber threats.

A profit with a purpose company, Nominet supports initiatives that contribute to a vibrant digital future and has donated over £45m to tech for good causes since 2008, benefitting more than 10 million people. The company has offices in Oxford and London in the UK and Washington D.C in the U.S.

Nominet's Cyber Security Solution – NTX

NTX will reduce risk on your network and eliminate threats before they cause harm.

All networks rely on DNS traffic. It is a critical source of information to check for threats and monitor the health of a network, but often overlooked in the security stack. NTX analyses network DNS traffic for both known and unknown threats. Embedding our patented algorithms means we eliminate threats from the network and identify zero-day activity not seen by traditional methods of detection. This narrows the window when malicious activity can compromise your network.

While best practice suggests that security should be considered at the planning stages of digital transformation initiatives, Nominet's NTX platform can be installed at any point in a project and deliver the same immediate protection to devices, systems, and data. This can be exceptionally useful in cases where it has not been possible to consider security at an earlier stage.

Eliminate network threats before they cause harm

Our continuous R&D efforts create powerful insights to predict, detect and block network threats.

Proven & trusted cyber security services

Protecting enterprise customers and chosen by UK Government.

Contextualise your network and know what good looks like

Understand normal network behaviours and identify any abnormal trends.

Threat hunting & forensics

Granular data capture to provide meaningful insight for the duration of your service.

Easy deployment & integration

With minimal touchpoints and rich APIs for your existing security investments.

NOMINET

For more information on how Nominet can help secure your business, please contacts us on:
UK: +44 (0)1865 332 255 | USA: +1 202 821 4256 | cybersecurity@nominet.uk | www.ntxcyber.com