

Driving the digital revolution:

A guide for boards



In partnership with



Contents

Letter from Governance Institute of Australia Chair	1
Research process and participants	2
Working group participants	2
Survey and survey respondents	2
Executive summary	5
Introduction	6
Setting a digital strategy	7
What is a digital transformation?	8
A lack of technology skills in the boardroom	10
Unease makes directors risk averse on cyber	10
Getting the right technology skills around the table	11
Executing digital strategy	13
Driving digital transformation	14
The impact on employees and customers	14
Regulation and data management	15
Managing data risk	15
Risks and opportunities	18
Conclusion	20
A roadmap for boards to navigate the digital revolution	20



A national membership association, Governance Institute of Australia advocates for a community of more than 43,000 governance and risk management professionals, equipping our members with the tools to drive better governance within their organisation. We tailor our resources for members in the listed, unlisted and not-for-profit sectors, and ensure our member's voice is heard loudly. As the only Australian provider of chartered governance accreditation, we offer a range of short courses, certificates and postgraduate study to help further the knowledge and education of the fast-growing governance and risk management profession. We run a strong program of thought leadership, research projects and news publications and draw upon our membership of the Chartered Governance Institute to monitor emerging global trends and challenges to ensure our members are prepared. Our members know that governance is at the core of every organisation — and in these tumultuous times, that good governance is more important than ever before.



Diligent is the pioneer in modern governance. We empower leaders to turn governance into a competitive advantage through unparalleled insight and highly secure, integrated SaaS applications. Diligent helps organisations thrive and endure in today's complex, global landscape. Our trusted, cloud-based applications streamline the day-to-day work of board management and committees. It supports collaboration and secure information sharing throughout the organisation, manage subsidiary and entity data, and deliver the insights and information leaders need to mitigate governance deficits and outperform the competition.

Letter from Governance Institute of Australia Chair

We are delighted to share with you Governance Institute of Australia's major thought leadership project for 2022 — *Driving the digital revolution: A guide for boards*.

There is no doubt, technology is the great business accelerator of our times prompting innovation, fast information flows and flexibility.

But technology also comes with a raft of hazards and risks — and is changing rapidly.

And as this report shows, many directors still have some hurdles to clear before they are leading, rather than observing, the digital revolution that is currently underway.

One of the most worrying findings in our survey was that 21 per cent of respondents do not have a digital transformation underway at their organisation, and 40 per cent of those respondents say it is not a priority.

But no business can thrive — or survive — without fit-for-purpose technology.

No business can be truly customer-centric and provide valued customer experience without fit-for-purpose technology. No business can really enable maximum staff efficiency and job satisfaction without fit-for-purpose technology. No business can succeed without the ability to interrogate its own data or without using AI because that is what provides essential insights into future customer behaviour and needs.

It is well known that a company's digital strategy is the way it can manage the 'S' in ESG risk. For example, the implementation of technology can have a significant impact on the nature of internal roles. Any digital strategy must model and plan for these changes so staff can be retrained and redeployed and taught how to adapt.

Technology can enable the oversight of stakeholder views, and risks such as modern slavery which are also part of the 'S' in ESG risk.

As our report states, a digital transformation is no longer a nice to have, and the risks of falling behind can be catastrophic for the organisation and thus destroy value. No board wants this. A sincere thank you to Diligent, the sponsors of this thought leadership, for recognising the urgent nature of these issues.

We recommend you use this report as a roadmap to ensure you are on track, to identify where greater innovation is required and to help you take charge of your digital revolution.



A handwritten signature in black ink that reads "Pauline B Vamos".

Pauline Vamos

Chair, Governance Institute of Australia

Research process and participants

Technology issues are one of the greatest challenges boards of directors currently face. They have risen up the agenda following rapid rates of digital adoption during the COVID-19 pandemic.

Technology risks such as cybercrime and data privacy are top-of-mind for most directors and doing well in these areas can set a business apart. Despite this, technology skills are not being prioritised at board level, which leaves organisations exposed to digital risk and unable to innovate to get ahead.

This report, the next in our future-focused series, explores the core digital issues boards face and provides guidance on how directors can successfully navigate their organisation through the digital revolution, emerging in a stronger position than ever.

Three main areas of research were carried out to inform this report. We convened a working group of digital experts to discuss the technology issues boards are facing, conducted an extensive survey, plus reconvened our working group for a second session to consider the survey responses and reflect on the themes that emerged.

Working group participants

Ian Oppermann, Chief Data Scientist for NSW and Immediate Past President of the Australian Computer Society

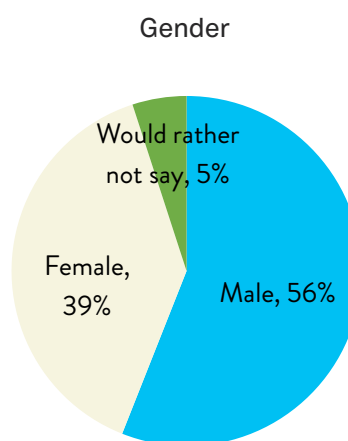
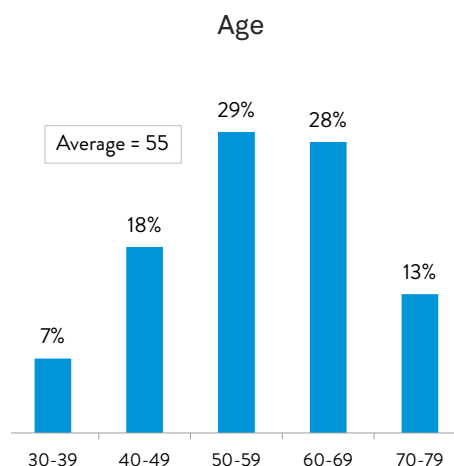
Dottie Schindlinger, Executive Director, Diligent Institute

Christoph Strizik, Chief Information Security Officer, Origin Energy and Member of the Amazon Web Services Global CISO Advisory Council

Peter Deans, Non-executive Director, RegtechAustralia and former Chief Risk Officer, Bank of Queensland

Kira Ciccarelli, Lead Research Specialist, Diligent Institute.

Respondent profile

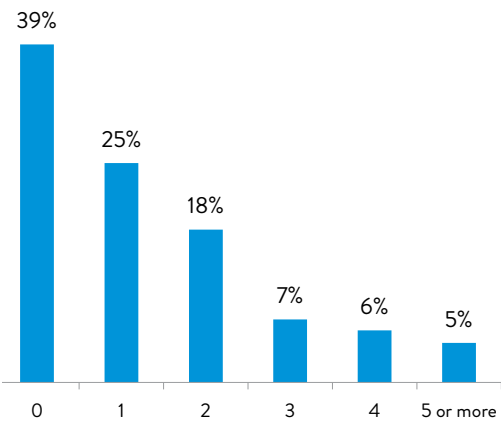


Survey and survey respondents

In May 2022 Governance Institute of Australia conducted an online survey of directors, company secretaries and other professionals. A total of 481 responses were received.

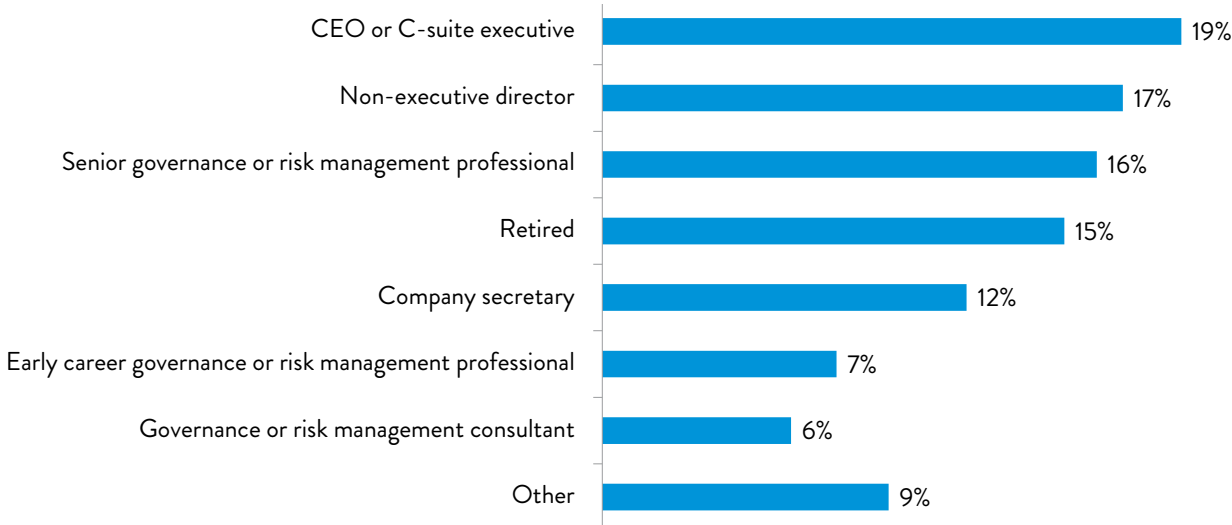
Board involvement

Number of board positions

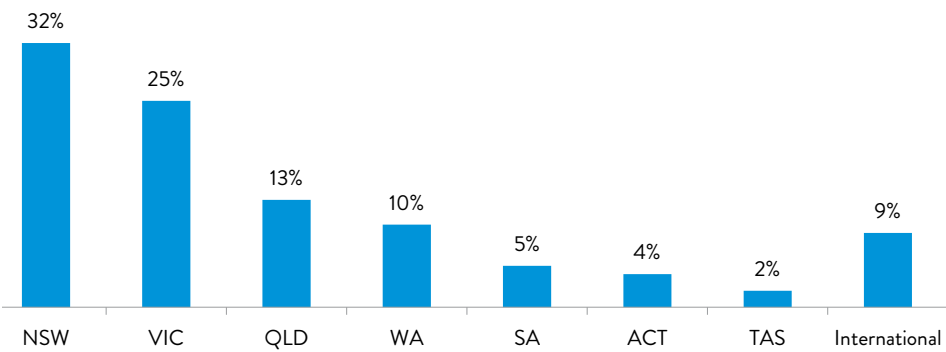


The average age of survey respondents is 55. Fifty-six per cent are male, 39 per cent are female and 5 per cent would rather not state their gender. Most respondents hold senior positions: 19 per cent are CEOs or C-suite executives, 17 per cent are non-executive directors, 16 per cent are senior governance or risk management professionals and 12 per cent are company secretaries. The majority of respondents don't hold a board position, 25 per cent hold one position and 18 per cent hold two positions.

Stage of career

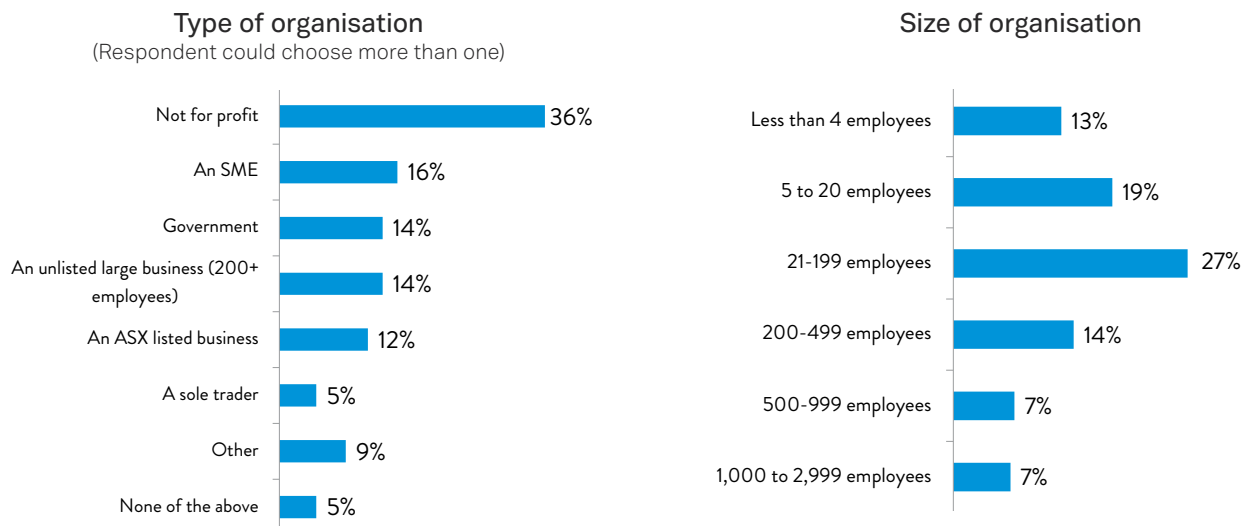


State based in



Most respondents are based in either New South Wales or Victoria and 9 per cent are based overseas.

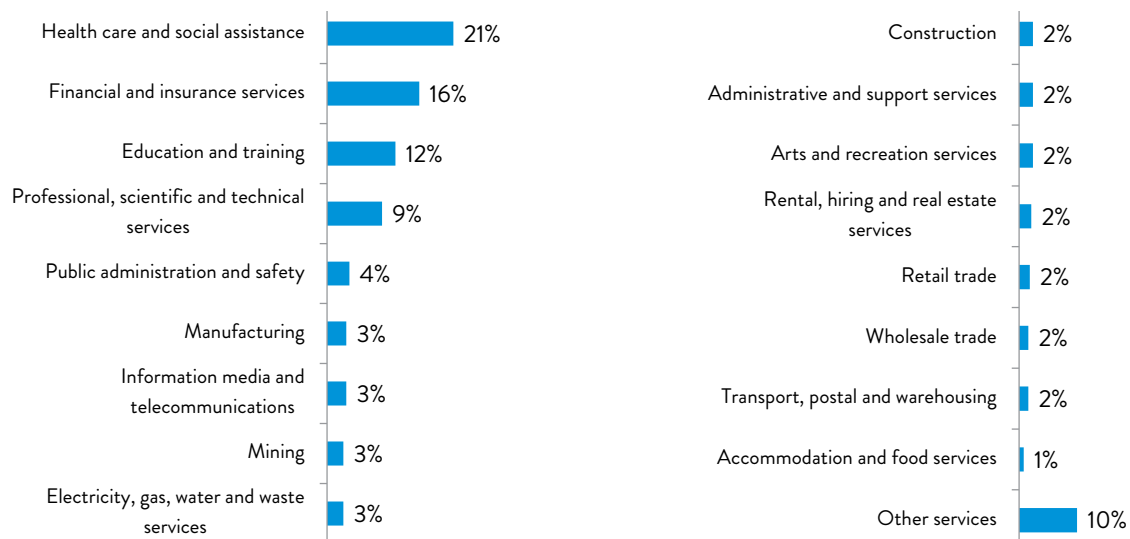
Organisation



A wide range of organisation types are represented. The highest proportion of respondents (36 per cent) work for a not-for-profit, 16 per cent are at a small-to-medium-sized enterprise, 14 per cent work for the government, 14 per cent are at a large unlisted business of more than 200 employees and 12 per cent are at an ASX listed business.

The most common organisation size represented is 21–199 employees (27 per cent), followed by 5–20 employees (19 per cent) and 200–499 employees (14 per cent).

Industry sector



A diverse range of industry sectors are also represented. Health care and social assistance is the most represented (21 per cent), followed by financial and insurance services (16 per cent) and education and training (12 per cent).

Executive summary

With all organisations now using technology to run — and differentiate — their business, digital transformation is no longer a nice to have.

Despite this, our survey found that some leaders have still not grasped the importance of digital and are failing to equip their organisation to deal with the technology challenges of the future. Our survey found that 21 per cent of respondents have no digital transformation underway and 34 per cent don't think their board is dealing competently with current technology challenges. Forty-six per cent rated their organisation average or poor when it comes to data management.

There's a lack of digital skills in the boardroom leaving directors ill equipped to probe digital strategy and feeling uneasy about technology risk. This unease makes directors risk averse on big issues like cyber security, which can stifle innovation.

Most survey respondents (93 per cent) think the board should be involved in technology issues. Despite this, 29 per cent don't think it's important for board members to have high level technology skills. The majority of respondents have few if any directors with digital skills on their board: 41 per cent say less than a quarter of their board members have technology skills and 13 per cent have no directors with digital skills.

Board directors need to upskill to meet the technology challenge and the nominations committee must ensure there is the right mix of skills on the board and keep this under review.

This report argues that innovation should be central to an organisation's digital strategy to ensure it creates a competitive edge. A narrow focus on digitising existing systems and processes is a missed opportunity. Only 33 per cent of survey respondents said their digital transformation currently involves strategic innovation and adaptation.

Cyber security and cyber attacks are considered the top technology risks for our survey respondents, both now and in 2030. This reflects the enormity, unpredictability and rapidly evolving nature of this area of risk and how vulnerable directors feel in the face of a threat that is so far out of their comfort zone.



In this context it's worrying that the report shows directors underestimate the risk of a ransomware attack. Governance professionals should educate their board on the significant damage a ransomware attack can do to a company, in some cases leaving it unable to recover.

The report finds data management has been overlooked in favour of cyber risk. Just under half of survey respondents (46 per cent) rate their organisation average or poor when it comes to data management.

The report highlights that overlooking data management could undermine a digital transformation and argues that this area needs to be prioritised. It's encouraging that 76 per cent of respondents have plans in place to improve their data management.

Our survey shows that the majority of respondents understand the need to develop and implement a digital transformation. This highlights the risk of falling behind, or even becoming obsolete, for organisations that haven't yet embraced technology. In a world where every business is a technology business, digital transformation is essential.

This report highlights the key issues directors should be considering when it comes to technology and the action they can take to press ahead on their digital journey.

Introduction

Boards are facing a deluge of data, increasingly sophisticated cyber attacks and a new crisis around every corner, all of which demand real-time information and new levels of nimbleness. The current economic climate underscores the need for boards to be able to adapt rapidly to changing circumstances.

The technology challenge directors are confronting intensified during the COVID-19 pandemic as organisations went through a rapid rate of digital adoption. The existing legal framework has been left struggling to keep pace.

In this context, it's clear that technology is one of the biggest challenges for boards and senior managers. It's not an easy challenge to address but doing so will be a core driver of success for organisations, enabling innovation and creating a competitive advantage.

If technology skills do not become a priority at the board table, directors will be left exposed and will struggle to steer their organisation through future challenges and opportunities.

Some businesses risk becoming obsolete if they do not undertake digital transformation. It's likely that most organisations will need to increase spending on digital transformation projects in the near to medium term.

Governance Institute's 2021 report, [Future of the board](#), found that technology disruption and cyber security risk will be among the top external challenges for directors by 2025. The report also identified technological know-how as one of the top three skills the future board member will need. In addition, it found that cyber security and data privacy, understanding the risk of new technology, and governance and compliance are set to be the major technological disruptors by 2025.

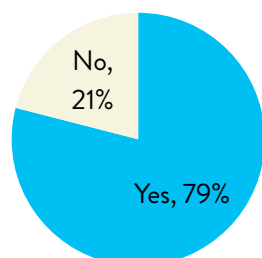
This report seeks to explore these themes in more detail to help directors understand how they can drive the digital revolution.



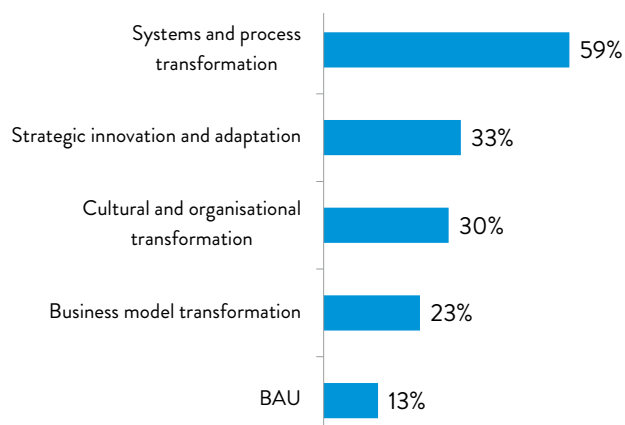
Setting a digital strategy

The prominence of technology

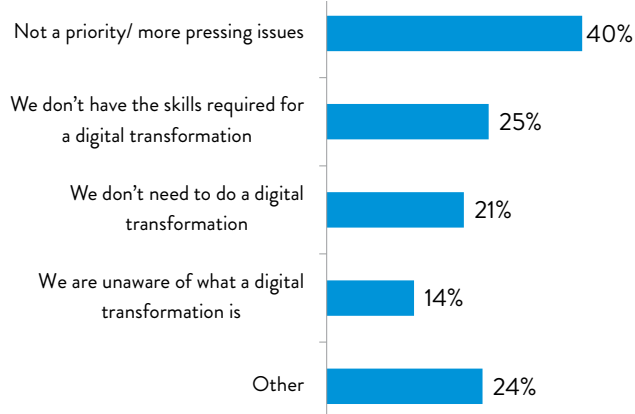
Is a digital transformation currently on your organisation's radar, or already underway?



If yes, at what stage is your organisation's digital transformation?



If no, why not?



The majority of survey respondents (79 per cent) said that a digital transformation was either underway at their organisation or on its radar. A significant 21 per cent said there was no digital transformation underway at their company.

The first working group convened for this report highlighted that some organisations have not yet developed a digital strategy. Its members stressed the importance of proactively agreeing and driving a digital strategy rather than allowing this area to evolve without appropriate oversight.

The largest proportion of survey respondents who are not undertaking a digital transformation (40 per cent) said it's not a priority for their organisation, or that their organisation faces more pressing issues. Twenty-five per cent of those not undertaking digital transformation say they don't have the necessary skills and 21 per cent believe they don't need to carry out a digital transformation. Worryingly, 14 per cent of those not undertaking a digital transformation say they are unaware of what a digital transformation is. Given it is good governance for organisations to embrace digital transformation and to articulate a technology strategy, this is cause for concern.

Of those already undertaking a digital transformation, the majority (59 per cent) are undertaking systems and process transformation and 23 per cent are undergoing business model transformation.

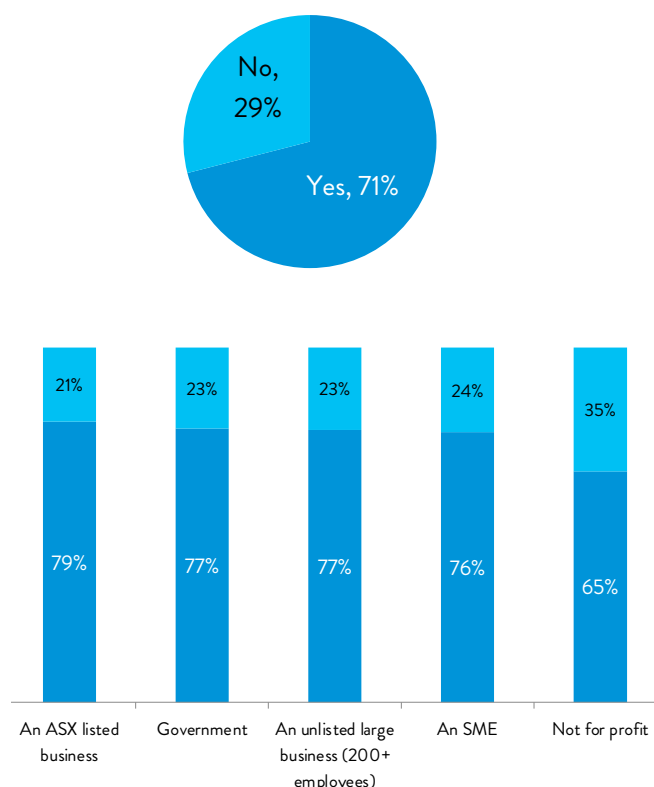
It's a massive opportunity lost if you just have a digital strategy to do the system and process upgrades that everybody else is doing anyway.

Christoph Strizik

Speaking at the second working group, Christoph Strizik highlighted that only 33 per cent of respondents said their digital transformation currently involves strategic innovation and adaptation. For him, innovation should be the cornerstone of a digital strategy that sets a business apart from its competitors. 'It's a massive opportunity lost if you just have a digital strategy to do the system and process upgrades that everybody else is doing anyway,' he argues.

The prominence of technology

Is your organisation's technology/digital strategy linked to the organisation's overall strategy?



Seventy-one per cent of survey respondents said their organisation's technology or digital strategy is linked to its overall strategy. This proportion was consistent across the different sectors represented.

What is a digital transformation?

Defining what digital transformation means is crucial but the meaning of digital transformation will vary depending on the organisation.

For some it will constitute fundamentally changing the business model to ensure survival. An example could be a book seller faced with the dominance of Amazon. Where this is the approach, the board will have to make the difficult decision to intentionally disrupt itself, which will feel risky.

For other organisations where the entire business model is not fundamentally threatened by the rise of technology, digital transformation could mean digitising processes or IT transformation. It could be about fully integrating technology throughout the business.

The first working group discussion observed that there is almost too much choice and too many ideas available to boards, which they need to weigh up and decide on.

The approach of board directors to digital transformation can vary from complete non-believers to progressive visionaries, with many shades in between. It's important to find a common language that enables all parties to communicate effectively when setting digital strategy.

Christoph Strizik argued at the working group that digital transformation should focus more on a change in mindset that goes beyond merely digitising processes. Widely available and cheap technology has changed the operating environment for businesses and lowered the barriers to entry for competitors. Organisations need to change their ways of working to reflect this shift, as well as using the data they gather to make better decisions and drive new product development.

The first working group highlighted partnering with third parties as a key aspect of digital strategy. Participants also stressed the importance of understanding the people who are driving technological change, for example customers and employees. The individuals overseeing the digital strategy should make sure they consult customers to understand what they want from the business. Multiple and thorough focus groups should be an important part of this process. It can be worth looking at how start-ups engage with their customers as an example of best practice and the level of energy that is required.



Questions directors should be asking about their digital transformation

What does a digital transformation look like for our organisation?

How does this interplay with other systems we already have in place?

Will it inhibit our ability to do the other things that we're doing?

Will additional time and effort be required to integrate it into existing systems?

Data security and privacy — are our policies up to standard?

Do we have the expertise on staff to be able to run this?

Build or buy?

How is this going to impact our current staff?

Whose job is going to change?

Do we need to make any redundancies, or hire more?

What sort of training do we have to do?

What's the impact of getting this right, or not getting it right?

What's the return on investment of our digital transformation?

What's in our software supply chain?

A lack of technology skills in the boardroom

Our survey uncovered a distinct lack of digital skills in the boardroom. Speaking at the first working group, Dottie Schindlinger observed, 'there still is a dearth of digital expertise in boardrooms.' She argued that directors might not feel confident addressing a complicated area they don't fully understand. Many board members feel they don't have a firm footing from which to push back and ask the right questions when discussing digital issues or digital strategy.

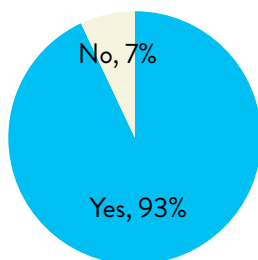
There still is a dearth of digital expertise in boardrooms.

Dottie Schindlinger

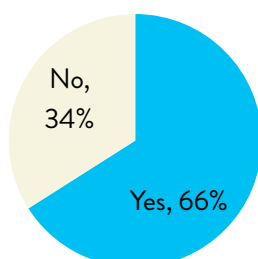
Many board directors take up their position after retiring from an executive role. Their experience may not be in tune with the demands of the modern customer or employee.

Technology and board

Should the board be involved in technology issues?

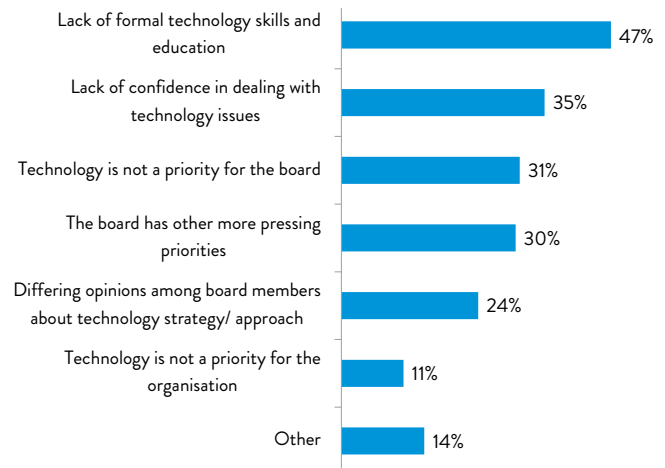


Is your board dealing competently with the organisation's current technology challenges?



Is your board dealing competently with the organisation's current technology challenges?

If no, why not?



Almost all survey respondents (93 per cent) agree that the board should be involved in technology issues.

However, 34 per cent of respondents don't think their board is dealing competently with the organisation's current technology challenges. For Christoph Strizik, this response is a major concern. He argues, 'every organisation is becoming a technology organisation to some degree...they are all using technology to run the business and differentiate the business.' Therefore, he believes, those boards that are falling short when it comes to technology are leaving their organisation ill prepared to sustain itself in the face of constant technological disruption.

Of those respondents who feel their board is not dealing competently with their organisation's current technology challenges, 47 per cent attribute this to a lack of formal technology skills and education, 35 per cent say it's because of a lack of confidence in dealing with technology issues and 31 per cent say that technology is not a priority for the board.

Despite this, it's encouraging that 66 per cent of respondents feel their board is dealing competently with the organisation's current technology challenges.

Unease makes directors risk averse on cyber

Directors' feeling of unease about technology feeds a risk averse approach to cyber security in boardrooms. Board members are overly wary about the potential for cyber attack because they don't feel confident about how to respond if their organisation were attacked. It's important to ensure the approach to cyber risk is realistic and doesn't negatively affect other areas of the business.



Our survey uncovered a distinct lack of digital skills in the boardroom.

Dottie Schindlinger

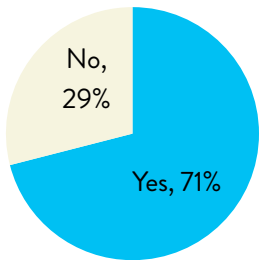
Speaking at the first working group, Dottie Schindlinger observed that directors are consistently more concerned about a cyber-related crisis than any other type of crisis, and this was true even during the COVID-19 pandemic. She said they ask, 'if a cyber event were to take out all of our systems on a day, would I know exactly what to do? Would I know how to respond and react in the moment?'

Survey respondents ranked cyber security and cyber attacks as the top current technology risks to organisations, which underlines the sense of unease in the boardroom over the potential for cyber attack.

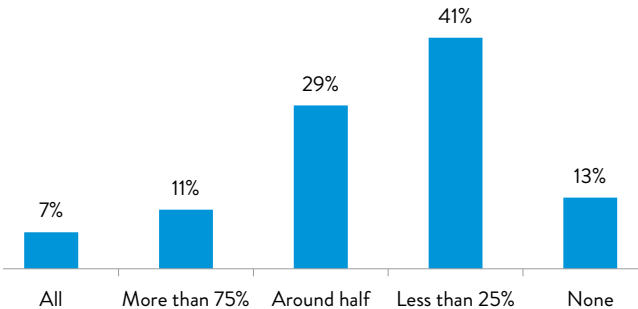
Getting the right technology skills around the table

Technology skills on the board

Is it important your organisation's board members have high level technology skills?



Among your current board members, how many have technology skills as part of their core skill set?



Seventy-one per cent of survey respondents agree it's important for their board members to have high level technology skills. A significant minority of respondents (29 per cent) disagree with this statement.

Forty-one per cent of respondents say less than a quarter of their board members have technology skills as part of their core skillset and 29 per cent say that around half of their board members have technology skills as part of their core skill set. Thirteen per cent say none of their board members have technology skills.

It's worrying that a significant minority of respondents don't see technology skills as a priority for board members and that some boards have no technology experts around the table.

If your board director cannot participate in the conversation because they have no grounding whatsoever [in technology] then you've really lost access to a real asset.

Ian Oppermann

Boards that don't have the right technical capability need to source it so that they are well equipped to discuss the risks and opportunities that digital presents.

Ian Oppermann argues that 'if your board director cannot participate in the conversation because they have no grounding whatsoever [in technology] then you've really lost access to a real asset. Or if they don't feel confident participating because they don't have that level of expertise, you've lost part of your collective...risk and responsibility taking [mindset].' For Oppermann, 'it's important to upskill enough in order to be part of the conversation.'

Oppermann also commented that, 'where the board doesn't have the technical capability, it needs to find that technical capability... and it needs to find a language and framework to say this is how we're going to quantify the level of risk we're willing to accept.'

But defining the perfect 'digital director' is difficult. There isn't a standardised digital skillset. For example, someone who's an expert in cyber security may not understand blockchain. For Kira Ciccarelli, not everyone will need to be a digital expert, but 'knowing what questions to ask of the right people' will be important.

It's essential to get the right overall mix of digital and technology skills in the boardroom. Nominations committees should bear in mind that in five years' time, the mix of digital skills the board requires will be very different to what is required now. To ensure they are on track though, the board could include an assessment of its digital skillset as part of its next board evaluation process.

Any training directors receive should be catered to their roles and responsibilities. This could include education and training on digital oversight, knowing how to ask the right questions of the right people within the organisation, and staying abreast of large-scale developments in the space.

Offering training that board members can undertake at their own pace, such as e-learning programs, can often work well because this format can be adapted to fit into directors' busy schedules.

Reputable universities are beginning to offer relevant courses to assist directors to learn more about digital strategy and technology. Working group member Peter Deans also suggests getting familiar with the processes being used by start-ups as a good way to get hands on with new technologies.

Another option could be to appoint a special adviser to the board to provide expertise in a particular area of digital or technology.

There is a clear divide between the size of an organisation and where they are up to with their digital journey. Peter Deans said that larger companies have already recognised the need to hire digital natives at the board and executive level who can develop the organisation's digital strategy. For him, the next challenge will be determining how the board embeds this new digital DNA throughout the organisation.

Also speaking at the second working group, Christoph Strizik agreed that part of the solution to a lack of digital skills in the boardroom will be appointing younger board members with very different backgrounds and experiences. He argued that the board as a whole will upskill naturally as a consequence of these board members being present.

Kira Ciccarelli agreed that there are an increasing number of directors with a technical skillset being appointed to boards, which should lead to a natural evolution in the board's understanding of digital issues. She also highlighted how the drive for greater overall diversity at board level will help to improve the board's digital skills because directors from underrepresented groups are less likely to have taken a traditional route to the boardroom.

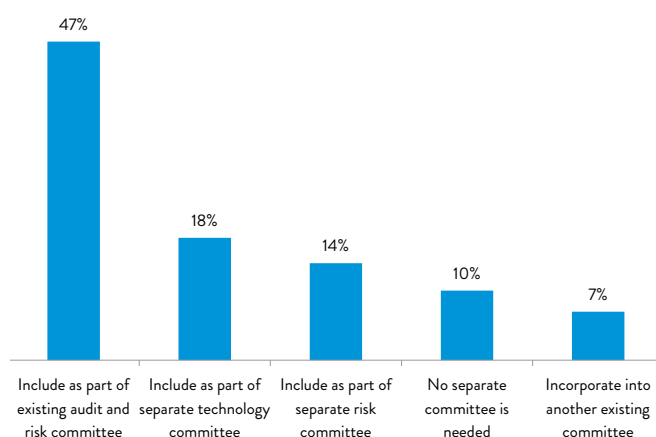
Being skilled in different ways of working could be as important as technical knowledge when it comes to implementing a successful digital transformation. For example, using agile working methods. Or iterative working, such as running small pilots to test how appropriate a certain technology is for your business, before rolling it out across the entire organisation.

Digital skills are also in demand across the entire workforce which in turn means digital is a key factor in the war for talent. Many organisations feel unable to deliver their digital strategy because of a skills shortage.

Executing digital strategy

When an organisation moves from developing to implementing its digital strategy, governance issues such as data privacy and cyber risk need to be addressed and managed.

The board and committee structure that is most effective for dealing with technology risk



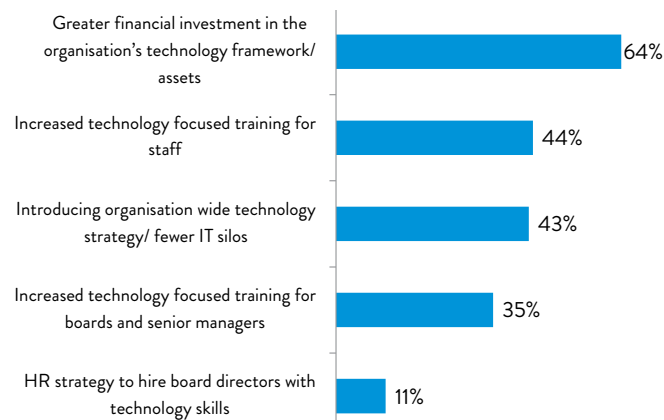
When it comes to managing technology risk, 47 per cent of survey respondents include oversight of this risk in the remit of the existing audit and risk committee. Eighteen per cent include it as part of a separate technology committee and 14 per cent include it as part of a separate risk committee.

In the future organisations may wish to place more emphasis on a separate technology committee to oversee digital strategy or digital transformation plans. This committee may also be required to monitor the involvement of third parties.

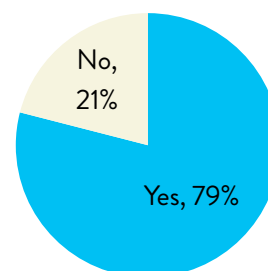
Speaking at the second working group, Peter Deans argued that more organisations should aim to have a separate technology committee at board level. He also noted that the task of monitoring technology risk is too great to be covered effectively as part of the broader remit of a combined audit and risk committee.

Dealing with technology risks

What action are you taking to deal with these technology risks?



Is 'technology risk' on your organisation's risk register?



In terms of the action organisations are currently taking to manage technology risks, 64 per cent of survey respondents say they are making greater financial investment in the organisation's technology framework or assets. Forty-four per cent of respondents have increased technology-focussed training for staff and 43 per cent are introducing an organisation-wide technology strategy with fewer IT silos.

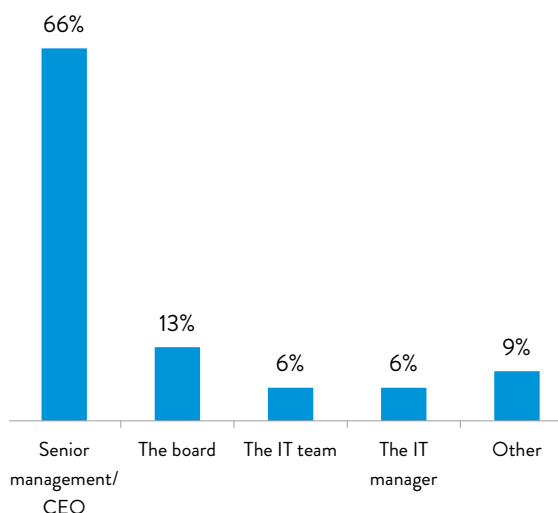
The majority of respondents (79 per cent) say technology risk is on their risk register.

The first working group discussion covered challenges such as how to include digital in key performance indicators (KPIs) and remuneration. A company could see an initial dip in income if it invests heavily in implementing a digital transformation, but this should lead to gains over the long term.

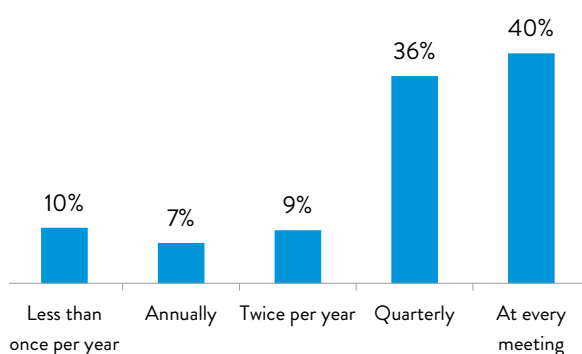
Driving digital transformation

It's important to think about the ownership of digital strategy. If this is spread across the organisation, there's a risk of duplicating effort, which can be costly. The board needs to be comfortable that the executive is collectively taking ownership of the digital strategy so that individual departments aren't left to build solutions that may not be fit for purpose.

Who has driven the digital transformation at your organisation?



How frequently do those responsible for the digital transformation report to the board?



Senior management or the CEO are currently driving the digital transformation at 66 per cent of survey respondents' organisations. A smaller proportion (13 per cent) say their board is driving their digital transformation. Given the lack of digital skills in the boardroom, it's perhaps not surprising that senior management is taking ownership of the digital transformation.

Respondents say those responsible for the digital transformation report on it to the full board either at every meeting (40 per cent) or quarterly (36 per cent).

Discussing these findings as part of the second working group, Peter Deans felt it was appropriate for the board to receive regular updates on digital transformation, with updates given at each board meeting a reflection of the business's imperative to undertake a digital transformation.

The impact on employees and customers

Peter Deans argues that the more employees and customers are exposed to, and benefit from, positive digital experiences, the more they will demand these kinds of experiences from the organisations they deal with. For Deans, 'this is the real driving force today behind digital transformation.'

The first working group expressed concern that the people side of technology strategy is often overlooked and highlighted how important it is to consider the impact of digital transformation on employees and customers. These areas are vital because they will have the biggest impact in terms of outcomes and delivery.

Dottie Schindlinger commented, 'Having that central focus of purpose and understanding the importance of the people that drive the technological change, the digital transformation itself, that [can be] the key to success.'

Ian Oppermann agreed that 'asking about impact on people is [important].' He commented, 'all businesses are ultimately people businesses so that's an important thing to do.'

Modern slavery is a lens that should be used when carrying out digital supply chain risk management. Ian Oppermann observed that often companies have identified modern slavery as a risk but don't have a real compliance framework in place to address this area, which can be very risky. He said he's unsure how widely people accept that modern slavery is a real issue.

Regulation and data management

Regulation of the digital space is playing catch up. It's attempting to address concerns that have been in the community for years. The first working group discussion considered that regulation can be quite blunt and certainly cannot be ignored.

The risks associated with non-compliance can be significant. Ian Oppermann commented at the first working group that regulation 'is the sort of thing that can really bite you.' The most noteworthy example is perhaps the European Union's General Data Protection Regulation (GDPR), which carries significant penalties for non-compliance. The regulation has a broad remit and [applies to](#):

- a company or entity which processes personal data as part of the activities of one of its branches established in the EU, regardless of where the data is processed; or
- a company established outside the EU and is offering goods/services (paid or for free) or is monitoring the behaviour of individuals in the EU.

The recently passed [Security Legislation Amendment \(Critical Infrastructure Protection\) Act](#) 2022 includes a new framework for enhanced cyber security obligations for operators of systems of national significance. These include:

- developing cyber security incident response plans to prepare for a cyber security incident
- undertaking cyber security exercises to build cyber preparedness
- undertaking vulnerability assessments to identify vulnerabilities for remediation and/or
- providing system information to develop and maintain a near-real time threat picture.

In Canada the House of Commons has also taken action to 'provide a framework for the protection of the critical cyber systems of services and systems that are vital to national security or public safety.' [The Critical Cyber Systems Protection Act](#) would require designated operators to, among other things:

- establish and implement cyber security programs
- mitigate supply-chain and third-party risks
- report cyber security incidents and
- comply with cyber security directions.

In the United States, the Securities and Exchange Commission (SEC) has [proposed amendments to its rules](#) 'to enhance and standardise disclosures regarding cyber security risk management, strategy, governance, and incident reporting by public companies' with the aim

of helping investors to evaluate public companies' cyber security practices.

According to the SEC, the proposed rule changes would require, among other things:

- current reporting about material cyber security incidents and periodic reporting to provide updates about previously reported cyber security incidents
- periodic reporting about a registrant's policies and procedures to identify and manage cyber security risks; the registrant's board of directors' oversight of cyber security risk; and management's role and expertise in assessing and managing cyber security risk and implementing cyber security policies and procedures
- annual reporting or certain proxy disclosure about the board of directors' cyber security expertise, if any.

Survey respondents ranked keeping up with changes in regulation and legislation as only the eighth most important technology risk organisations are currently facing. However, casting forward to 2030, respondents see this risk as the fourth most pressing technology risk organisations will face. This perhaps reflects an awareness that this area will require even more focus in future as the amount of relevant legislation increases and regulatory scrutiny intensifies.

Managing data risk

Getting data management right is critical in ensuring a smooth digital transformation process.

But as with cyber security, boards will need to strike a balance between keeping data safe and complying with relevant data privacy regulations and not locking data up to the extent that the opportunities it offers for the business can't be realised.

One way to manage data risk is to be selective and methodical about the data the organisation collects. Collecting more data than you really need creates unnecessary risk.

Minimising the amount of data you collect also gives you a better chance of being ethical in the way you use and manage it.

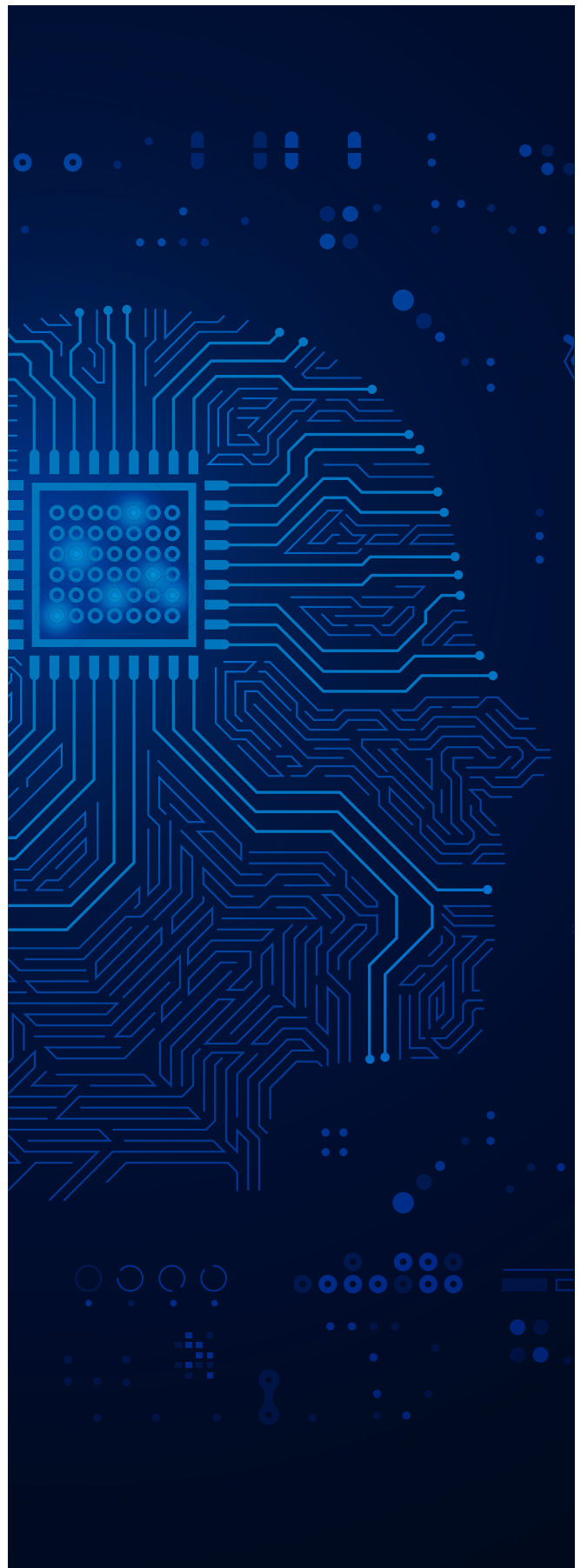
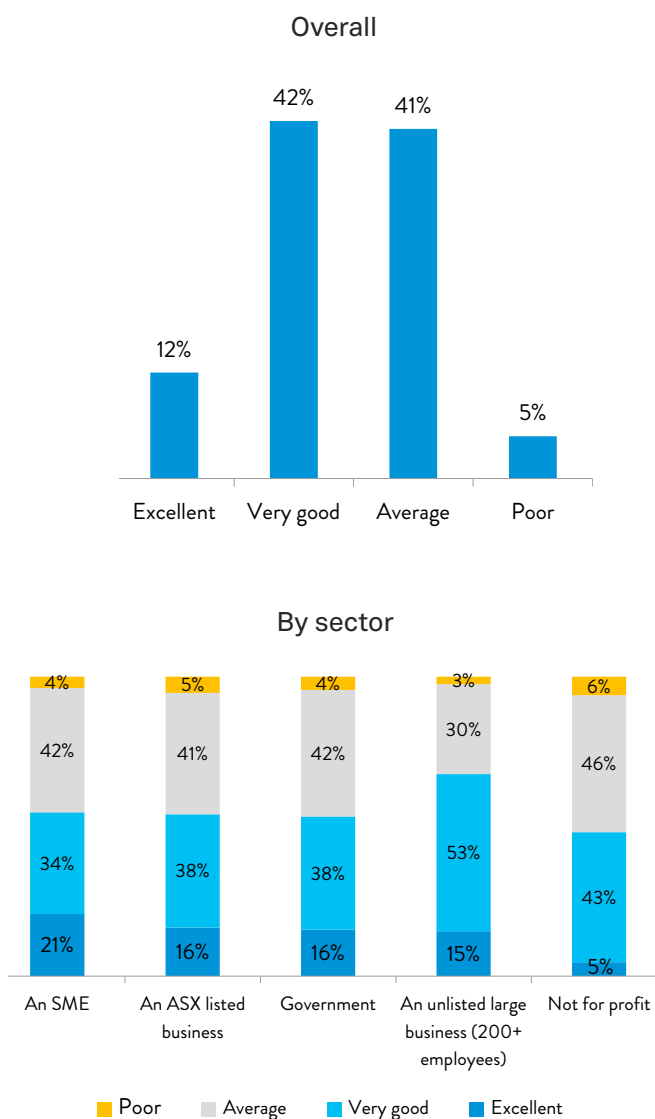
In the world of data I don't think we've got a good enough handle on what we mean by "personally identifiable information".

Ian Oppermann

Speaking at the first working group, Ian Oppermann said, “in the world of data I don’t think we’ve got a good enough handle on what we mean by “personally identifiable information”.” He argued that this lack of understanding leads to a risk averse approach to data handling meaning that organisations miss the opportunities that data presents for the business.

Also speaking at the first working group, Peter Deans argued that understanding the relevant data regulation, implementing it, and making sure it’s being adhered to should be part of the risk management remit. One approach could be to appoint a chief risk officer and then assign specific individual responsibilities for each regulatory requirement.

Rating of the organisation's management and protection of data



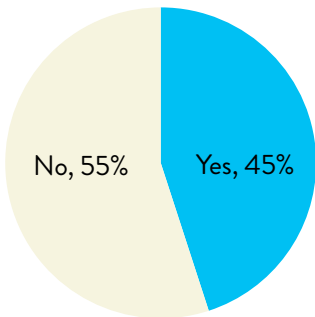
Survey respondents were split on the quality of their organisation's management and protection of data: 54 per cent rated their organisation excellent or very good in this area, but 46 per cent rated their organisation average or poor.

SMEs and ASX listed companies rated themselves higher than not-for-profits, which may reflect a greater amount of regulation applying to the former.

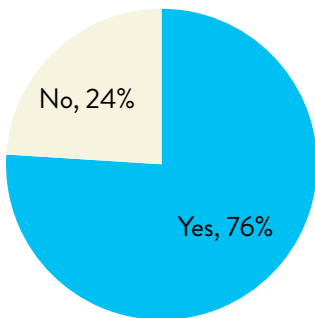
It's worrying that nearly half of respondents think their organisation is underperforming when it comes to data management. Peter Deans argued that data management has often been overlooked with cyber security and privacy risk seen as a more pressing issues for the board. He said that companies have collected a lot of data as a result of adopting new technological solutions but have not implemented the necessary data management systems to index and record this data in a sensible way. Given the amount of data that has been collected, it will be a huge challenge for companies to organise and catalogue it all. Deans highlights a lack of skills at board level on this issue as well, commenting that there's been 'an underinvestment in data governance.'

Data management

Is your board actively involved in data management challenges and issues?



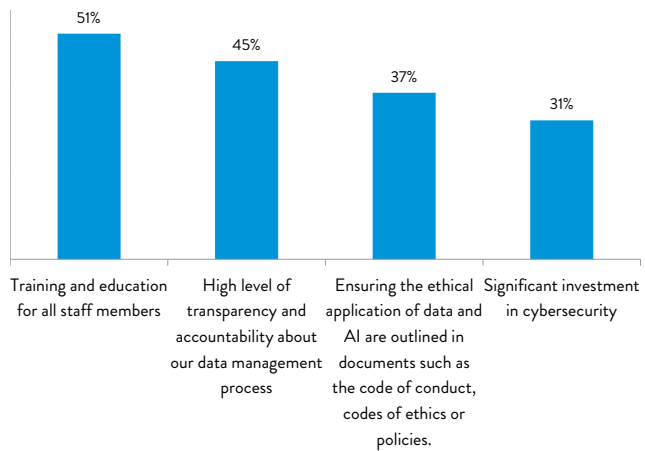
Do you have plans in place to improve your data management and protection?



The views of our survey respondents on data management issues reflect the argument that, to date, the board has not been significantly involved in this area. Just over half of the survey respondents (55 per cent) say their boards aren't actively involved in data management challenges and issues; 45 per cent say they are actively involved.

The majority of respondents (76 per cent) say they have plans in place to improve their data management and protection. This suggests that even where the board has been involved in data management, there is still room for improvement for a significant proportion of organisations.

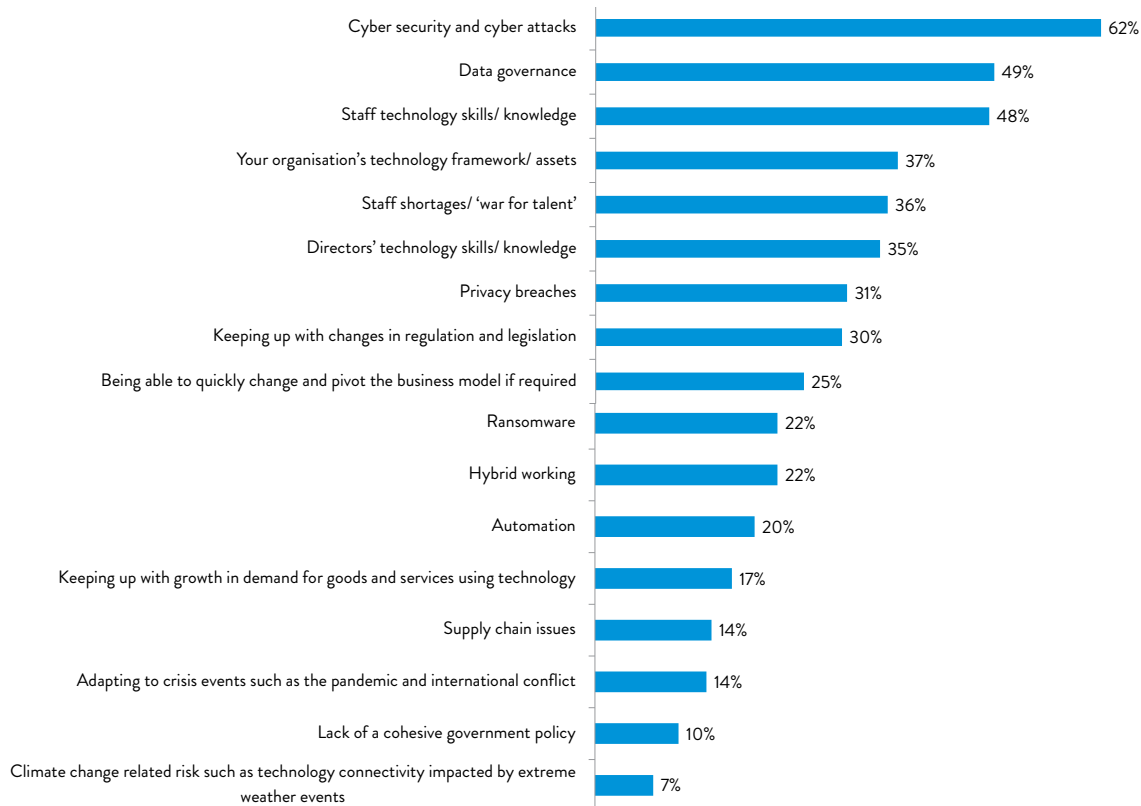
Steps organisation takes to ensure data and any AI is being used ethically



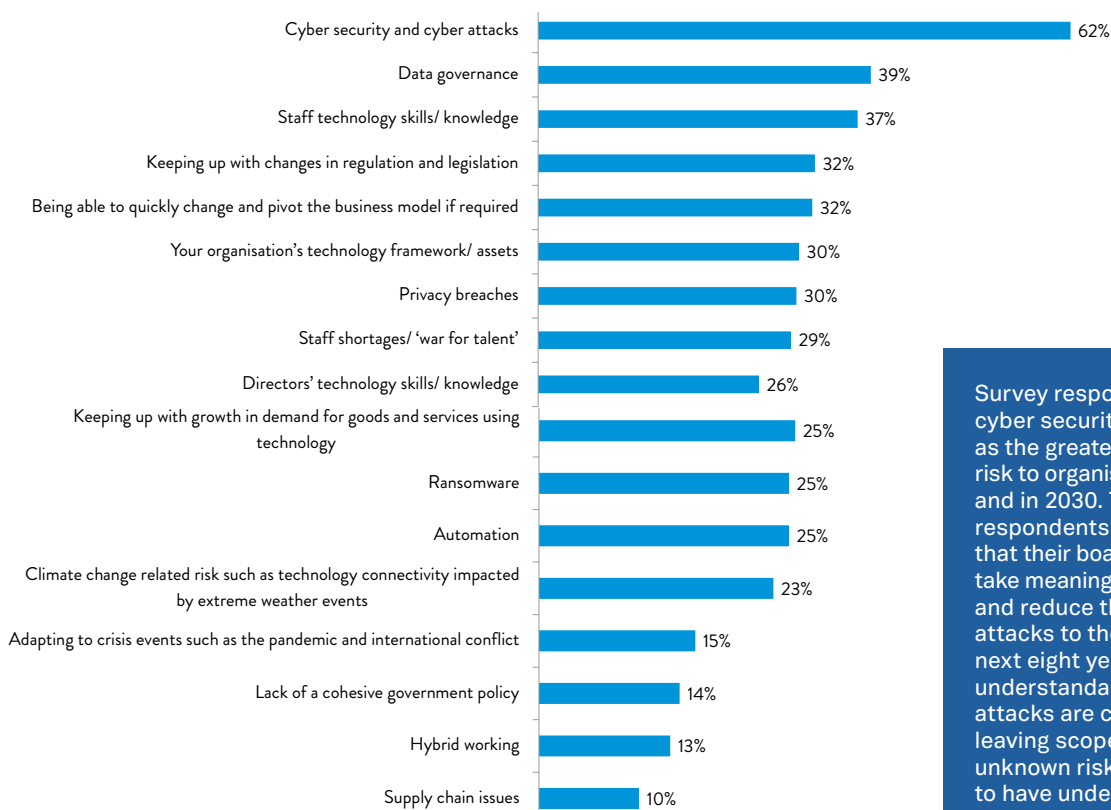
Around half of respondents (51 per cent) say they are training and educating all staff members to ensure data and artificial intelligence (AI) are being used ethically. A further 45 per cent said they are ensuring a high level of transparency and accountability around their data management processes and 37 per cent said they are ensuring the ethical application of data and AI are outlined in documents such as the codes of conduct and ethics as well as any relevant policies. Thirty-one per cent of respondents are making a significant investment in cyber security to ensure the ethical use of data and AI by their organisation.

Risks and opportunities

The current key technology risks to organisations



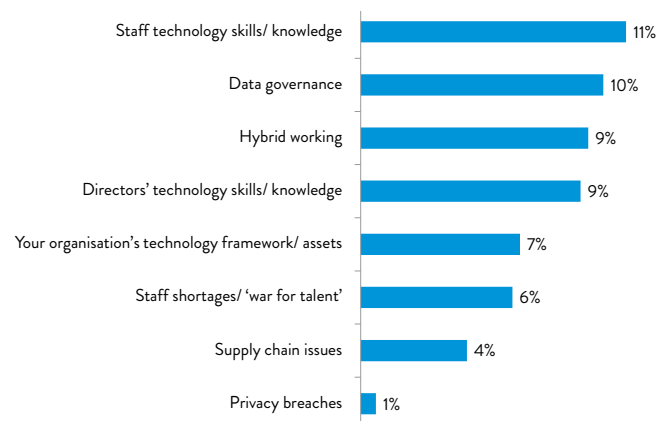
Expected technology risks to organisations in 2030



Survey respondents ranked cyber security and cyber attacks as the greatest technology risk to organisations both now and in 2030. This suggests respondents don't feel confident that their board will be able to take meaningful action to address and reduce the threat of cyber attacks to their business over the next eight years. This is perhaps understandable given how cyber attacks are constantly evolving, leaving scope for endless unknown risks the board needs to have under regular review.

Risks that are greater now than they will be in 2030

(The number is the % threat expected now minus the % expected in 2030)



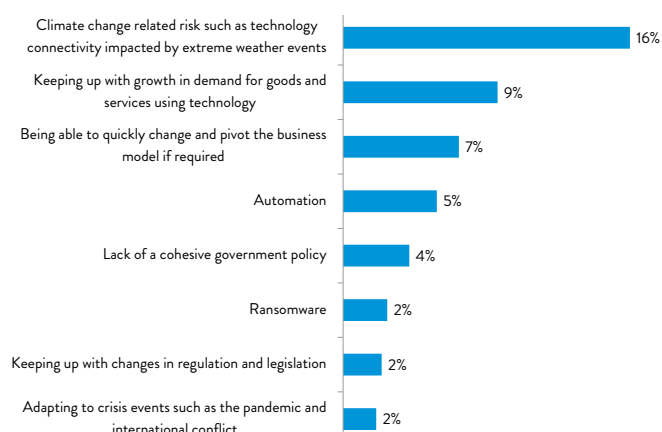
Survey respondents felt more positive about their ability to address the risks of staff technology skills and knowledge, data governance, and hybrid working, which they ranked as the top three risks that are greater now than they will be in 2030.

Despite this, respondents still ranked data governance and staff technology skills and knowledge as the second and third greatest technology risks to organisations in 2030, after cyber security and cyber attacks. This suggests there will be a lot of work to do to manage these risks both now and in the future.

Hybrid working is ranked second to bottom on the list of technology threats organisations will face in 2030. This suggests this risk is symptomatic of a certain moment in time coming out of the COVID-19 pandemic and that by 2030 organisations will have found ways to manage the risks associated with new ways of working.

Risks that will be greater in 2030 than they are currently

(The number is the % threat expected in 2030 minus the % threat now)



Survey respondents believe climate change-related risk such as technology connectivity impacted by extreme weather events will be greater in 2030 than it is now. This is perhaps part of a broader recognition of the wide-ranging effects that the climate crisis will have on every aspect of life by 2030.

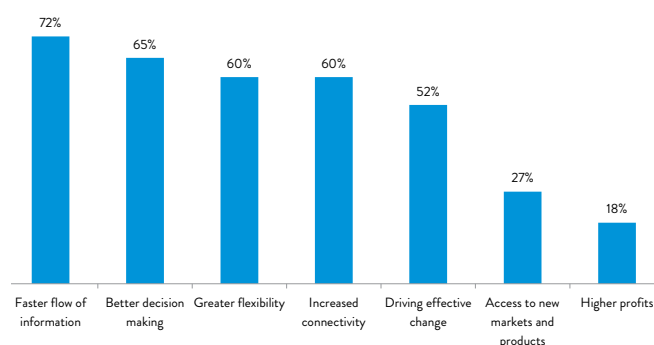
Ransomware is consistently ranked by survey respondents in the middle of the perceived technology threats that organisations face, both now and in 2030. Boards may not be placing enough emphasis on this common and often very effective form of cyber attack.

This might reflect a lack of awareness of the potentially devastating effects of a ransomware attack on a business: how quickly it can do significant damage, becoming almost an existential threat to the business. It can also be difficult to recover from a ransomware attack, taking weeks or months. Some organisations never recover from a ransomware attack. The working group felt the realities of ransomware and how it can affect a business may need to be made more explicit to boards to ensure they give it the attention it requires.

Opportunities

Technology risks should be balanced against the opportunities that digital technology offers, for example to grow a business and to innovate.

The greatest benefits of technology



Survey respondents ranked faster information flow as the greatest benefit of technology (72 per cent), followed by better decision-making (65 per cent), greater flexibility (60 per cent), increased connectivity (60 per cent), and driving effective change (52 per cent).

Conclusion



The risks of overlooking digital transformation are significant, which means it is particularly worrying that many organisations have still not begun their digital journey. However, most survey respondents agree that digital transformation is necessary and are at least taking some type of action to make it happen. Remaining resistant will only leave organisations struggling to keep pace, or perhaps threaten their very existence.

Technology offers an opportunity for innovation that can give a business a competitive edge. Digital strategy should therefore focus on innovation to maximise its benefits for the business. There are also opportunities for directors to learn new digital skills or deepen their understanding of technology, which they should embrace to ensure they too remain relevant and of value to their organisation.

It's important for directors to place digital transformation in a broader context and understand its implications for the people related to the organisation. In many ways customers, shareholders and employees are the real drivers of technological innovation because they will demand better and more varied opportunities for digital engagement with the company.

It's vital for the board to identify who's responsible for executing digital and cyber strategy in their organisation and be in regular contact with them. While directors can read and self-teach on wider developments in the cyber and digital world, it takes regular, thorough communication with digital leaders at their organisation, both in and outside board meetings, to understand how the company fits into larger trends, and how they can best take advantage of risks and opportunities.

The following roadmap outlines a plan for directors to drive the digital revolution at their organisation, empowering innovation which will in turn help ensure they are best placed for the future.

A roadmap for boards to drive the digital revolution

- **Embrace digital:** it's good governance to undergo a digital transformation
- **Define your strategy:** know what digital transformation means for your organisation
- **Innovate:** make sure innovation is at the heart of your digital strategy
- **Upskill:** make sure you have the right mix of technology skills around the boardroom table
- **Focus:** establish a board-level technology committee to oversee your digital transformation
- **Discuss:** make digital transformation a standing agenda item for each board meeting
- **Don't fear cyber:** keep cyber risk and mitigation processes under constant review to build the board's confidence
- **Get on top of data:** establish data management systems to mitigate risk and facilitate your digital transformation.

[Click here to see the Survey Snapshot.](#)



Governance Institute of Australia Ltd

Level 10, 5 Hunter Street
Sydney NSW 2000

T (02) 9223 5744
E info@governanceinstitute.com.au
W governanceinstitute.com.au

ACN: 008 615 950
ABN: 49 008 615 950