Moneyweb

Soapbox

Navigating a disruptive force

Like it or not, digitalisation is intrinsically linked to pretty much everything.

Lionel Moyal, Michael Judin and Robbi Laurenson / 31 January 2019 12:00 No comments so far

Which is worse – the top two business risks (business interruption and cyber incidents), or the fact that 65% of consumers surveyed said they cut ties with a brand over a single poor customer service experience. Picture: Shutterstock

"The 21st century has been characterised by fundamental changes in both business and society. These fundamental changes provided the context within which the King Committee set out to draft King IV and have influenced both its content and approach." – Mervyn E King SC, chair emeritus of the King Committee

Business and society have both faced unprecedented change in the 21st century, intensified and magnified by the rapid evolution of the digital age. These fundamental changes are so intensely disruptive that organisations need an effective and integrated strategy, enabled by digital, to be sustainable. By extension, the formulation of a digital-enabled strategy has become a critical prerequisite of an organisation's implementation of the principles of King IV.

The changes happened fast. Less than 12 years ago, in 2007, Apple released its first-generation iPhone, the culmination of only a few decades of evolution of the information age. At that

moment, mobile and cloud technologies converged, and the digital age suddenly became much more real for businesses and consumers.

Today, disruption continues to accelerate, with developments in cloud computing, artificial intelligence (AI), robotics, blockchain and the internet of things (IoT). The rapid pace of change makes it difficult for most organisations to stay ahead. Consider that in this era, a company remains on the American Standard & Poor's 500 index for an average of just 20 years, compared to its peak of 100 years around 1937. In 2018, seven of the top 10 publicly traded companies were software platform companies, compared to only one in 2008.

So how do organisations think about this?

King IV is a significant evolution from King III in that it links governance more tightly to value creation and the achievement of desired outcomes defined as Good Performance, Ethical Culture, Effective Control as well as Trust, Reputation and Legitimacy. No longer can this responsibility merely be delegated to a single CEO or IT department. Digitalisation is intrinsically linked to all aspects of an organisation and should be the accountability of the entire governing body. As such, company directors and committee members have a fiduciary duty in terms of the Companies Act to seek clarity on the impact of digitalisation on their organisation, and to manage it accordingly.

Aligning the digital strategy with the outcomes and principles of King IV

Organisations today face common challenges – including becoming more customer-led, improving speed to market, creating a culture that attracts talent and uncompromising focus on governance, compliance, cybersecurity and privacy.

Each of these challenges can be effectively addressed through digital transformation in specific areas of an organisation.

Modernise the workplace

At the core of an organisation's ability to transform is the engagement and empowerment of its employees. Gallup reports the average engagement among employees across organisations worldwide at only 15%. Visionary leaders are significantly improving their levels of employee engagement and enhancing productivity and organisational performance. Workplace modernisation is a logical place to start the digital journey, as improving employee engagement ultimately leads to improved customer experience. For this reason, it is a foundational pillar for good performance. It also directly supports each of the outcomes of King IV.

As a start, each employee should be given a digital identity forming the basis for digital engagement with the company. Information workers are generally the forerunners in this process. For information workers, workplace performance has shifted from personal to team productivity, enhanced by platforms for communication and collaboration. But while some of this transformation is taking place naturally, it is often not prioritised. Many leaders still see employee engagement as a nice-to-have rather than a critical business function.

The priority placed on digitalisation to enhance employee engagement is starting to shift with the appearance of new generations of leaders. Generation Xers (born mid 1960s to 1980) and millennials are equally digitally savvy (54% for GenX versus 56% for millennials, as reported by the DDI Global Leadership Forecast 2018) and are more likely to embrace digitalisation as a key way to ensure performance and sustainability.

Customer experience

In a study on the state of customer service by Parature in 2014, 65% of 1 000 consumers said they have cut ties with a brand over a *single* poor customer service experience.

Today's consumers and business users alike expect their service providers to value their time and have become accustomed to enhanced customer experiences.

With the increasing prevalence of platforms for digital engagement, customers have come to expect more responsive and personalised services across multiple channels. Putting the customer at the centre is just the start. Being able to develop deep insights on each of its customers allows an organisation to anticipate its customers' needs and challenges. Data analytics and omni-channel customer engagement platforms enable a competitive advantage by pairing digital experiences with human advice.

The demand for more personalised self-service is being met with the use of intelligent conversational interfaces such as chat bots. According to Gartner, "by 2020, the average person will have more conversations with bots than with their spouse". The creation of chat bots has become so simple that even non-technical users can create their own and make them available on any of the most commonly used social platforms in existence (such as **QnA Maker** from Microsoft).

Operational efficiencies

Driving growth in existing customers and in new markets is only one part of ensuring a profitable and sustainable business. The other critical factor is reducing costs and realising operational efficiencies. Technology plays a significant role in streamlining business processes. Take automation through robotics, IoT technology and AI for example.

Wikipedia defines the IoT as the network of physical devices, vehicles, home appliances, and other items embedded with electronics, software, sensors, actuators, enabled to connect and exchange data. This creates opportunities for more direct integration of the physical world into computer-based systems, resulting in efficiency improvements, economic benefits, and reduced human exertion. By 2020, the IoT market is expected to reach $457 billion, with 73% of companies surveyed in 2016 actively investing in IoT (Keystone Strategy, 2016).

Even more impactful is the prevalence of AI, which exists across applications from smart phones to self-driving cars and is now appearing in everyday business software. The advances in AI are possible because of the exponential growth in data available from digital sensors and

devices, combined with the use of machine-learning algorithms that can learn and make predictions from data through pattern recognition, feedback loops and outcome prediction.

AI in the workplace has significant benefits to operational efficiencies but could have a significant human impact. Repetitive and routine task-based work is likely to be replaced by AI-driven processes and robots, hence the urgency attached to accelerating skills development in the workforce. The World Economic Forum Future of Jobs Report 2018 estimates that 54% of employees will require significant reskilling and upskilling by 2022 and predicts that up to 75 million jobs could be displaced globally, made up of large-scale declines in some roles offset by the potential creation of up to 133 million new roles.

Privacy

An organisation is the custodian of personal information about its employees, customers and suppliers and must ensure that this information is securely stored and managed and a respect for privacy cultivated across all systems, processes and interactions.

In 2018, the General Data Protection Regulation (GDPR) came into effect in the European Union (EU). It imposes rules on companies that offer goods and services to people in the EU, or which collect and analyse data tied to EU residents. Many countries are following suit. In South Africa, the Protection of Personal Information (PoPI) Act is due to come into effect around 2020.

In terms of GDPR and PoPI, organisations must adopt transparent policies and implement controls, systems and training. This includes data collection and retention policies as well as timeous notifications to authorities on data breaches and security to deal with the increasing risks of cyber threats.

From an information technology perspective, this implies that an organisation must ensure that appropriate policies for data classification are enforced across its own and third-party systems. Fortunately, tools are available to automate data discovery and classification based on machine learning rules and detection of personally identifiable information. Modern email and cloud-based communication, collaboration and information management platforms implement native support for data classification and controls for managing private information. At the same time, obsolete systems and processes that were not designed with privacy and security in mind must be assessed and modernised or replaced to mitigate any inherent risks.

Cyber security

According the Allianz Risk Barometer, the top two business risks for 2018 were business interruption and cyber incidents (42% and 40% respectively). South Africa is reported to have the third highest number of cyber crime victims worldwide, losing billions a year to cyber attacks.

Only a few years ago, protecting an organisation from cyber threats simply required securing the perimeter by establishing a firewall controlling all data connections to and from the internet, supplemented by anti-virus software. Today, data is spread across internal systems, cloud-based platforms and mobile devices, and shared with employees, suppliers and customers. In

addition, devices that can be compromised include not only computers and servers but also mobile devices from different manufacturers running a myriad of operating systems, network appliances, printers, scanners, vehicles and virtually any device containing a programmable microchip.

In the words of Cisco CEO John Chambers: “There are two types of companies: those that have been hacked, and those that don’t yet know they have been hacked.”

A study by FireEye in its M-Trends report of 2018 showed that the median number of days an organisation is compromised before discovering a breach is 101 days.

Guidance for governing bodies is therefore to ensure that data is adequately classified and protected where it rests, and that tools are used to monitor unusual patterns of data flow and user behaviour, identify threats quickly, and mitigate their impact.

Security can no longer operate as a siloed IT function, but rather as a fundamental business process.

This extends also into the human element. Many breaches are the result of simple mistakes by employees opening malicious links or attachments, or not following security policies. Executives and members of boards are often targeted, raising the importance of user training to ensure appropriate levels of awareness and responsibility.

Thus, applying effective control as per King IV necessitates an approach that recognises the shift in an organisation’s risk profile as it progresses through its digital transformation.

Trust, transparency and ethical culture

In 2016, the Facebook platform enabled Cambridge Analytica to illicitly harvest personally identifiable data from up to 87 million people. Cambridge Analytica used this information to target political messaging to users during Donald Trump’s presidential campaign. Trust, reputation and legitimacy are fundamentally impacted by an organisation’s ability to maintain a clear stance on privacy and ensure transparency in how digital assets are managed. This implies establishing, adhering to and reporting on a policy on the collection, usage, protection and disposal of data.

Beyond the risks related to privacy and cyber security, an organisation’s legitimacy is impacted by its conscientious approach to transformation, commitment towards employment retention and skills development, and contribution to social investments. This is important not only for an organisation’s own employees but also for the wellbeing of the economy.

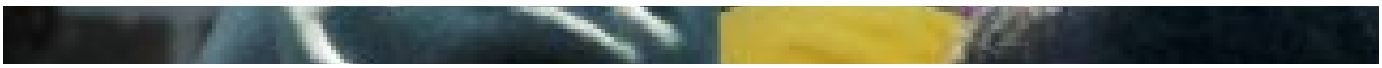
The core tenets of King IV are to lead ethically and effectively, govern in a way as to create an ethical culture, and govern so as to be a responsible corporate citizen. Equally important is to ensure digital responsibility and transparency by embedding ethical principles in data privacy, compliance, automation, and AI policies.

Conclusion

Today almost every business is a digital business and a competitor is likely to emerge from an entirely different domain.

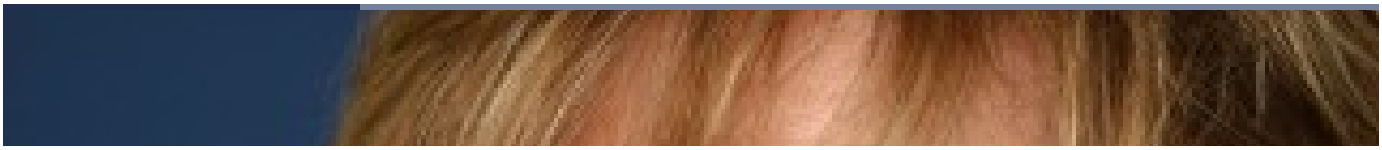
With this blurring of the lines between industries, organisations have an inherent responsibility to understand the opportunities and risks that come with digital transformation. Perhaps the most compelling outcome for an organisation is the formulation of a bold business strategy that is enabled by digital and aligned with the principles of King IV.

Lionel Moyal is office business group lead at Microsoft SA and Michael Judin a senior partner at Judin Combrinck Attorneys; with input from Robbi Laurenson, digital transformation advisor at Microsoft SA.



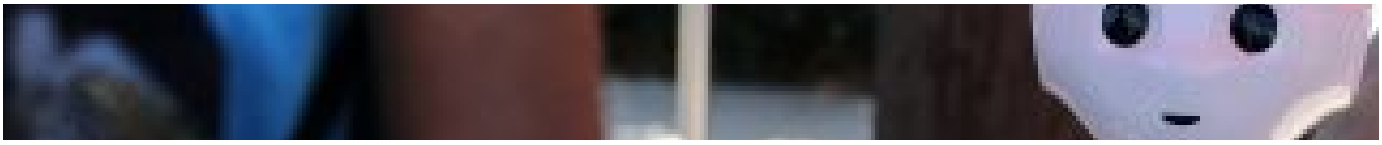
Zimbabwe vice president reportedly returns to SA for treatment

LATEST OPINION



After the revolt, who will pick up the pieces?

The impact of US policy on emerging markets: Three investor misconceptions



Artificial Intelligence in the world of tax