VOLUME 1

IDC's

DX Insights

MAKING SENSE OF DIGITAL TRANSFORMATION & THE NEW REALITIES FOR BUSINESS

CLOUD – THE CATALYST FOR TRANSFORMATION

IDC
Analyze the Future

IN COLLABORATION WITH

IDC
Analyze the Future

www.idc-cema.com
Tel: +971 4 391 2741
Fax: +971 4 391 1922

FOREWORD

Digital transformation (DX). While many use the term synonymously with going digital or simply using digital solutions, we at IDC believe that it goes way beyond that. For DX is not limited to the boundaries of IT.

It is about much more than IT bringing in solutions to streamline or automate processes; it is about the transformation of business. Ultimately, DX involves leveraging technology to create alternating customer experiences and open up new revenue streams, all while using information to drive competitive advantage.

What truly makes DX a reality is the synergies between IT and the business. At IDC, our traditional focus has been on engaging with CIOs around the use of IT within their organisations. Over the past few years, however, these same CIOs have increasingly cited a rise in IT and business alignment, with collaboration growing across the organisation as part of a combined effort to improve overall competitiveness.

Given this rise in synergies across the enterprise, IDC has partnered with *Gulf Business* to create a series of supplements that will provide both IT and business leaders with valuable insights into the current state of digital transformation in the region. We will also look at how business leaders are engaging in the procurement of so-called 3rd Platform technologies (ie, cloud, mobile, big data, and social).

In this first edition, a number of senior IDC analysts will guide you through the DX landscape as they explore the trends that will shape the future relationship between line-of-business leaders and the IT department. We also shine a spotlight on Saudi Arabia's National Transformation Program (NTP) and examine the evolution of infrastructure and the use of cloud by lines of business.

There are fascinating insights from the supply-side of the industry too: Dell EMC discusses the emergence of DX in the region and highlights Etisalat Misr's successful use of hybrid cloud to drive operational efficiencies; Akamai explains how effective cloud security can protect networks and create a more resilient organisation; and Fortinet offers advice on creating a more integrated security strategy as emerging technologies increasingly gain traction within the modern digital enterprise.

To compete with the true digital pioneers of this world, organisations must be prepared to experiment with emerging technologies, embrace open and integrated ecosystems, and embed innovation into the very fabric of the enterprise. DX is here to stay, and it will continue to reshape traditional industries as we know them. Our aim at IDC is to make sure you don't fall behind.

JYOTI LALCHANDANI
Group Vice President & Regional MD
IDC Middle East, Turkey & Africa

TRANSFORMING YOUR BUSINESS TO THRIVE IN THE DIGITAL ECONOMY

By **Jyoti Lalchandani** – Group Vice President & Regional MD – IDC Middle East, Turkey & Africa

As the so-called '3rd Platform' technologies of cloud, mobility, big data, and social become more firmly entrenched across the region, a new band of innovation accelerators are lining up to transform the very fundamentals of how we do business. These digital game changers include the likes of 3D printing, wearables, robotics, cognitive systems, next-gen security, virtual reality, and the rapidly growing Internet of Things.

The task of incorporating these digital technologies into the very fabric of enterprise processes in order to drive new revenue streams and previously unimaginable efficiencies sits at the heart of a process that has become known as 'Digital Transformation'. At IDC we define digital transformation as a continuous process by which enterprises adapt to or drive disruptive changes across their external ecosystems of customers and markets.

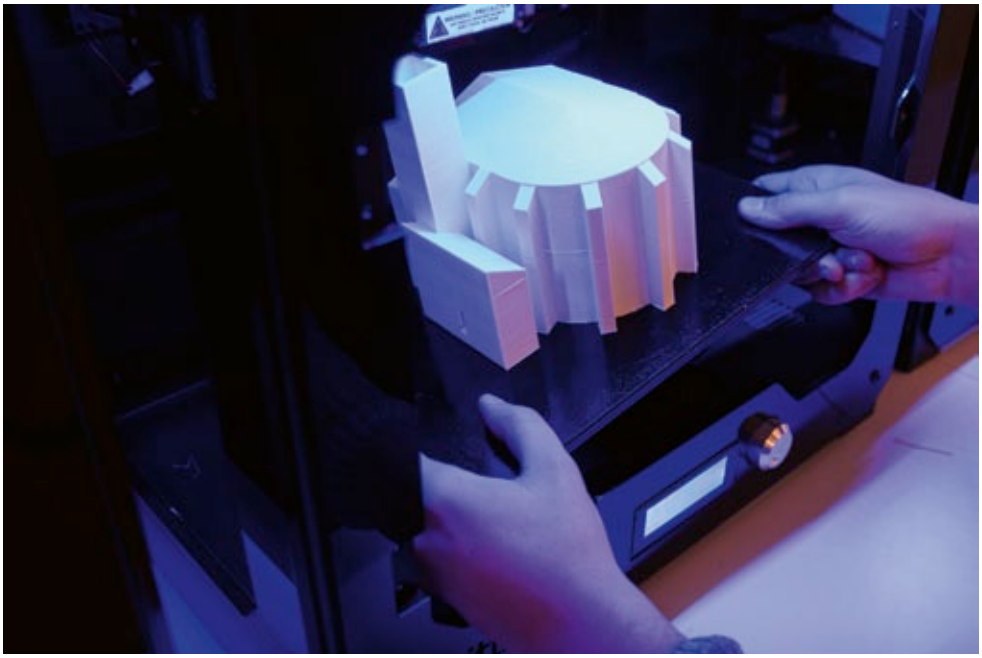
And while you might not know it yet, digital transformation is occurring all around us every second of every day, disrupting customers, business models, and even entire industries as it goes. Whether a business is using technology to better engage with its customers and suppliers, utilising new business models to keep pace with the explosive rate of change, or simply creating new strategies that rely on technology to accomplish day-to-day tasks, it has already taken its first steps

towards enabling digital transformation.

At IDC we believe the single most important competency required to thrive in this new digital economy is the ability to rapidly respond to changing conditions within the ecosystem in which the organisation resides. And while warnings of impending change are nothing new in an industry that is driven by innovation, the current rate of change we are seeing within the ICT space is truly unprecedented.

As such, digital transformation is a foregone conclusion for most, if not all, businesses. It's a process that simply has to take place to some degree in order to secure future profitability. And the stats certainly back this assertion up. Each year, Forbes magazine releases its 'Global 2,000' ranking of the top 2,000 public companies in the world, and IDC predicts that by next year, 66 per cent of them will have placed digital transformation initiatives at the center of their corporate strategies. By the following year, we expect 75 per cent of them to have deployed 'digital twins' of their products/services, supply networks, sales channels, and operations, and by 2020, we believe the deployment of digital technologies will have improved the success rate of new products by as much as 70 per cent.

With this in mind, the choices at this point in time are to entrench and hope for the best; develop digital transformation competencies and become a disruptor; or split the difference and become a follower. Given



these choices, IDC believes that CIOs should look to align their IT activities with the pre-requisites for true digital transformation by improving the customer experience and pursuing digitally enabled products and services.

They should shift their focus away from short-term internal operations to longer-term external projects, and also look to reduce the amount of time they have to spend on driving IT service availability, cost reductions, and business process optimisation. In this regard, it is important that CIOs look to maximise the time spent on innovative activities aimed at creating new IT services, improving the time to market, and increasing revenue.

Broadly speaking, I see digital transformation occurring across five key elements of the forward-thinking enterprise – leadership, information, operating models, worksource strategies, and the provision of a truly omni-channel customer experience. The extent to which digital transformation is embraced across these five critical areas means that enterprises can be split into resisters, explorers, players, transformers, and disruptors. And if you're not at least exploring these exciting new opportunities by now, you may have already missed the boat.

This journey requires commitment across all levels of the enterprise, because simply dabbling in digital initiatives will not get an organisation where it needs to be in order to compete with the lean and lethal digital start-ups that are gearing up to steal market share. For that reason, I strongly recommend the implementation of an optimised, end-to-end digital transformation strategy that is targeted at helping the organisation to work faster, lead smarter, and win the inevitable talent wars. Those organisations that embrace this approach and become true digital transformers will find themselves much better positioned to outwit their competitors and deploy solutions that reduce the risk and increase the reward.

Just about every operating unit of every corporation has already been disrupted by emerging digital trends in one way or another, and this process is only going to intensify over the coming years as more and more businesses figure out how to transform emerging digital technologies into reliable digital revenue streams. With the rewards on offer including the ability to innovate faster, operate more efficiently, and connect with customers in real time, there has simply never been a better opportunity for the region's organisations to scale up their digital initiatives and secure that all-important competitive advantage.

THE JOURNEY TO MAKING DIGITAL TRANSFORMATION A REALITY

With digital transformation now critical for organisations looking to remain competitive and relevant, IDC sat down with **Mohammed Amin**, Dell EMC's senior vice president for the Middle East, Turkey, and Africa, to find out more.

IDC: Much has been written about the ongoing digital revolution. Where do you think the Middle East stands in this regard?

MA: We find ourselves in a time of unprecedented change – a time which many have described as the next Industrial Revolution, a time where customers are increasingly looking to transform themselves into digital businesses. And this is particularly true here in this region.

This transformation is as much about the business as it is about technology, with organisations using digital solutions to create entirely new operating models, experiences, revenue opportunities, and value. And in this regard, the Middle East is not just making a mark for itself in the world of digital business, it is leading the way.

IDC: So how would you summarise the current state of digital transformation in the region?

MA: A recent research study commissioned by Dell EMC shows that only 33 per cent of Middle East companies feel they are able to facilitate innovation in an agile manner, and only 27 per cent are actively investing in digital skills; additionally, 4 per cent of the businesses surveyed in the region are capable of acting digitally and almost half (45 per cent) of them fear they may become obsolete in the next three to five years due to competition from digital-born start-ups.

These statistics suggest that companies in the region are still trying to grasp how to embed emerging technology strategies into business operations and value chains in order to become more agile – which forms the core foundation of becoming digital-ready.

At Dell EMC, we believe that change brings rich opportunities. And alongside our partners, we are well positioned to provide the essential infrastructure for organisations to build their digital future, shift the status quo, transform IT, and protect their most important asset – information.

IDC: What changes are you seeing in the way that organisations address their IT infrastructure needs?

MA: A lot of our customers are modernising and transitioning

their datacenter models and strategies to adopt cloud-native capabilities, using infrastructure that facilitates granular and agile growth through converged and hyper-converged solutions as well as hybrid cloud. And given the ever-increasing pace of emerging digital and technology trends and opportunities, our customers are looking for partners that can help enable their digital transformation in dynamic ways.

The interesting thing about new IT trends today is that they are more holistic in nature than ever before (ie, they scale across infrastructure stacks and break the silos of operation). Digital transformation aggressively targets an increase in business technology capability while simultaneously targeting a reduction in complexity and cost. Our customers recognise that simplifying their partnerships with technology vendors and service providers is crucial to facilitating the latter. End-to-End systems, solutions, and service providers are critical 'consultants' for customers looking to engage in digital transformation today.

IDC: How should IT infrastructure evolve to support digital transformation initiatives?

MA: It takes an agile and flexible organisation to compete and win in today's aggressive and dynamic business landscape. Technology that delivers high levels of scalability and reliability can ensure an organisation's success in a digital Middle East. However, ageing legacy system, inhibit innovation instead of enabling it across many business functions.

As such, IT infrastructure needs to accelerate the cycle of innovation and create competitive differentiation. To do this organisations need to modernise their datacenter infrastructure, automate their IT processes, and transform their operating models to advance their digital transformation journeys.

Dell EMC enables organisations to succeed in their digital transformation plans and strategies with a unique end-to-end capability across infrastructure, services, and consulting. As the only end-to-end IT vendor in the industry, we provide strong capabilities in the fastest-growing areas of the industry, including hybrid cloud, software-defined datacenter, converged infrastructure, platform-as-a-service, data analytics, mobility, and cybersecurity.

IDC: How can organisations more proactively manage their transition to using cloud?

MA: The region continues to boast some of the most ambitious initiatives for transforming community living and driving economic diversity. From Saudi Arabia's National Vision 2030 to Smart Dubai initiatives here in the UAE, the choice of underlying cloud-powered infrastructure is instrumental to ensuring that businesses and communities leverage new 'smart' ways of living. Technologies like hybrid cloud offer the perfect middle ground, extending the powerful blend of public cloud flexibility and agility together with the security and protection of a private cloud to create the reliable performance-backed architecture that our nations need to continue introducing innovative systems and services.

First and foremost, organisations wanting to transition to using cloud should proactively look for solutions that fit their needs, rather than the other way around. Infrastructure that allows for flexible scale-up and scale-out while converging the management of various workloads and protocols ensures growth can be controlled while services are managed and delivered separately.

IDC: How can Dell EMC help in this regard?

Dell EMC gives customers an unprecedented level of innovation and choice of solutions and partnerships for deploying hybrid clouds. Our customers are able to incorporate the best of both public and private cloud strategies and empower IT to become a broker of trusted cloud services. The result is a hybrid cloud solution capable of supporting traditional and next-gen applications, as well as greater financial transparency so IT can prove its value to the business and the introduction of a seamless and secure management experience.

Dell EMC's Enterprise Hybrid Cloud is built on our converged and hyper-converged infrastructures, providing enterprises of all sizes with flexible deployment choices as the foundation for infrastructure-as-a-service. It allows organisations to deliver IT-as-a-service to meet their specific business needs, so IT can start delivering value to the business faster than by building a fragmented platform. Dell EMC also brings professional services for every step of the cloud journey, along with one-contact support.

IDC: What challenges are organisations in the region facing in terms of their cloud investments?

MA: Although organisations in the region are generally embracing the move to the cloud, they are facing challenges in areas such as data preparation for conversion to cloud; integrated cloud/non-cloud management; backup, archiving, and disaster control strategies; and the need to address security and trust concerns.

As such, there is growing interest in adopting advanced hybrid cloud models to transform delivery of IT services and thereby combine the control, reliability, and confidence of private cloud with the simplicity, flexibility, and cost efficiency of public cloud.

IDC: Why is it important for the 'business' – and not just IT – to understand the advantages of cloud and agile infrastructure?

MA: The use of hybrid cloud and agile infrastructure are imperatives for success in the digital age. Failing to deliver in such a highly contested marketplace could trigger the beginning of a digital crisis. Digital transformation enabled by hybrid cloud and agile infrastructure helps organisations increase IT agility and makes implementing digital business initiatives a faster, easier, and less expensive process.

Furthermore, by reducing IT costs, hybrid cloud and an advanced, agile infrastructure enables investment in digital transformation. According to the findings of a survey commissioned by Dell EMC last year, organisations with a significant number of hybrid cloud workloads are three times more likely to be approaching their digital business and infrastructure readiness goals than non-adopters.

INFRASTRUCTURE REQUIREMENTS FOR DIGITAL TRANSFORMATION

By **Swapna Subramani** – Senior Research Manager, Enterprise Systems- IDC Middle East, Turkey and Africa

The Middle East enterprise infrastructure market has been undergoing a metamorphosis in parallel with digital transformation (DX) initiatives. The adoption of 3rd Platform technologies like cloud, mobile, social media, and Big Data and analytics is reshaping the datacenter and pushing organisations to reassess their datacenter architecture.

In IDC's CXO Study 2017, which surveyed 240 C-level executives across verticals in the Middle East, 68 per cent of respondents said their organisations had launched DX or were planning to start the process in 2017. The Middle East is thus at a critical juncture in the DX journey. Enterprises will require improved computing power, data processing capabilities, connectivity, and real-time interfaces to realise the full potential of their initiatives.

Enterprises undergoing DX face several key challenges. IDC's survey found that C-level executives in the Middle East are concerned that DX could lead to conflicting priorities within their organisations. They are also concerned about investment requirements, particularly the need to invest in improving their base IT systems, including infrastructure.

Datacenter infrastructure is evolving alongside the demands of business and DX. As DX advances, the datacenter must become both increasingly agile and manageable. Server, storage, and networking vendors are creating an enhanced set of offerings that will attract datacenter operators looking to move to the next level of infrastructure efficiency within their DX platforms.

DX initiatives will require newer, consolidated systems with centralised administration capabilities. The datacenter will be impacted by the development of private clouds, adoption of flash, infrastructure convergence, and a shift to software-defined architectures.

PRIVATE CLOUD

The Middle East has seen a surge of private cloud implementations over the last few years. According to a survey conducted at IDC's Middle East CIO summit 2016, 41 per cent of CIOs in the region planned to implement private clouds in 2016–2017. In 2016, more than 12 per cent of infrastructure spending was expected to be dedicated to private, public, or hybrid cloud buildouts. This figure is expected to rise to more than 25 per cent over the next five years. This will require infrastructure to be increasingly agile and responsive.

FLASH

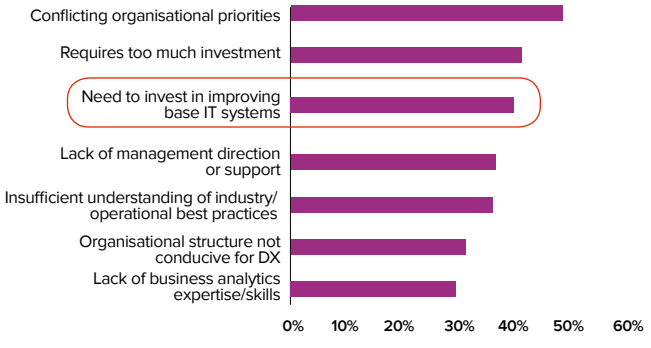
Flash technologies have seen a strong uptake over the past three years in the Middle East. The explosive increase in data from DX initiatives is the biggest catalyst necessitating dynamic and scalable storage innovation. As the price per gigabyte for solid state disks and hard disk drives converge, flash is becoming the go-to storage solution for a variety of workloads that are part of a digitally transforming organisation.

INFRASTRUCTURE CONVERGENCE

Software-defined architectures, converged systems, and hyper-converged infrastructure will play key roles in reshaping the datacenter. Hyper-converged solutions not only enable hardware consolidation, they also allow vendor consolidation, thus easing IT management complexities. These systems enable simplified administration and operations via a single user interface. Because of their modular nature, they also offer the ability to scale out.

An organisation's adoption of new products, solutions, and services as part of a DX journey should be carried out holistically, with a strategy aimed at simultaneously transforming business processes, the datacenter, and the IT framework. With DX embedded in the organisation, IT should be deployed as an enabler. Each business process should be integrated with IT, and the resulting data should be used to enhance operational processes. The underlying infrastructure is the key factor that will facilitate integration. The goal is a seamless, consolidated, and converged infrastructure that is both software-defined and cloud-enabled. Such infrastructures will eliminate bottlenecks, boost efficiencies, and accelerate an enterprise's DX timeline. They will form the core of DX aspirations in the Middle East in the coming years.

Challenges in DX transformation



SOURCE: IDC CXO ME SURVEY, 2017

ACHIEVING EFFICIENCIES WITH HYBRID CLOUD

A Dell EMC case study

THE CLIENT

Etisalat Misr is one of Egypt's leading telecommunications providers and offers consumers across the country access to the fastest broadband internet connection in the market in addition to a mix of industry leading services. Since its launch, Etisalat Misr has maintained a position of technology leadership in the Egyptian market, serving millions of customer with the best quality of products and services.

THE CHALLENGE

With a clear focus on enhancing customer satisfaction through improved service offerings and delivery, Etisalat Misr sought to revolutionise its IT backbone powered on IT-as-a-service capabilities that would enable the agility and efficiency required to support its ambitious growth trajectory.

THE SOLUTION

Etisalat Misr selected the Dell EMC Federation Enterprise Hybrid Cloud to seamlessly extend its private datacenter into the public cloud, using the same tools and processes it already had in place, without adding costs or complexity to the existing environment.

Built on a combination of industry-leading Dell EMC and VMware technologies, the new solution enables the IT team at Etisalat Misr to create a single platform to effectively manage both traditional and next-generation applications. With ViPR Controller, Etisalat Misr can now enable new storage-as-a-service capabilities to optimise costs and storage without adding unnecessary managerial complexity.

Adding Dell EMC VNX-F mid-range flash storage to the mix further enabled Etisalat Misr to power application performance to aid availability and service delivery.

THE APPROACH

Senior business and IT consultants from Dell EMC Global Services helped define the right cloud vision for Etisalat Misr. This was achieved by assessing the company's current IT capabilities, establishing the rate of change the IT organisation could sustain, and providing a cloud strategy that met the specific needs of the business.

THE RESULTS

Following the implementation, Etisalat Misr enjoyed these benefits:

- **Optimised cloud delivery model:** The Dell EMC Cloud Advisory Service helped Etisalat determine cloud application placement, define cloud architecture to deliver IT as a service, build the business case, assess the readiness for service automation, and develop a transformational roadmap for business and IT.
- **Enhanced service delivery:** The Dell EMC Hybrid Cloud self-service portal allows users to provision new storage, backup, database, and platform services, enabling IT teams to focus more on innovation than on the provision of service and support.
- **Increased efficiency and transparency:** Storage automation through ViPR Controller has improved storage utilisation and significantly reduced operational time. VMware VCloud Automation Center simplifies management while driving greater cost transparency.
- **Improved performance:** The implementation of VNX-F has enabled Etisalat Misr to improve application performance by 300 per cent and has significantly reduced database response time from 8-10 minutes to sub-millisecond speeds.
- **Greater agility:** Etisalat Misr's IT teams are now able to provision a blend of private and public cloud environments to support current business applications while enabling the scale for developing next-generation applications for the future.

DELL EMC

THE FUTURE OF IT-LOB RELATIONSHIPS

By **Ranjit Rajan** – AVP, Research – IDC Middle East, Turkey & Africa

As digital transformation (DX) spreads rapidly across various industries, the influence of line-of-business (LoB) executives on technology procurement is undergoing a major shift. Cloud, mobility, big data, and social business — together with innovation accelerators such as cognitive systems, the Internet of Things (IoT), robotics, augmented and virtual reality, 3D printing, and next-gen security — are driving a new wave of business process transformation and, in many cases, business model transformation. With such high stakes, LoB units are increasingly staking a claim for greater influence in technology initiatives.

In most organisations in the Middle East, digital initiatives are being increasingly funded by line-of-business departments or jointly funded by IT and the LoBs. This is a fundamental change from the days when the IT department was solely responsible for procuring, provisioning, and supporting technology in the organisation. In this context, the relationship between the IT function and LoBs is expected to change rapidly over the next few years. Here are a few observations on the trends that will shape this relationship in the future.

Innovation at the Business End

Many organisations, particularly in the financial services, retail, telecommunications, and public services sectors, are focusing much of their digital efforts on transforming customer omni-channel engagement. Here, the LoB teams that are at the forefront of customer engagement, such as sales, marketing, and customer service departments, are emerging as natural internal champions for digital initiatives. Although the project teams for such initiatives consist of both LoB and IT personnel, increasingly, the project managers are being appointed from the LoBs. The LoBs are also increasing their funding in these areas and, very

soon, will overtake spending by the IT department. IT's primary responsibility is to then enable an agile infrastructure — increasingly, in a cloud model — to support the digital solutions at the front end.

Disruption in the Back Office

Technology is poised to disrupt back-office functions. Cognitive systems and robots will accelerate intelligent automation of finance, procurement, and administrative processes. Waves of business process automation over the years have led to a plethora of enterprise applications; however, while this new wave of intelligent automation will lead to a much greater increase in productivity, it will also have serious implications for jobs, skilling, and corporate culture. The influence of CFOs and COO on intelligent process automation decisions will be significant, as they have far-reaching consequences. IT will, of course, play the role of facilitator and enabler, but it will be challenging for the average IT function to adequately advise on and enable such non-traditional technologies, and thereby be a leading partner in such projects.

Data-Driven Innovation

Traditionally, the IT department has played the role of custodian of corporate digitised — mostly structured — data. But with the explosion in the number of devices and applications, and the deluge of data — mostly unstructured — passing through the organisation, IT departments are struggling to control it. Storing, securing, and analysing the data requires a more formidable information management architecture. With all the digitised data available, LoBs are now realising the value of data as an asset, providing it can be adequately analysed and leveraged to improve business processes. Furthermore, many organisations are beginning to find ways to monetise the data assets they possess and generate new revenue streams from this data. Consumer products, retail, and telecommunications companies are leading the way in this initiative. The revenue-generation opportunity from data will prompt LoBs to not only take greater ownership of the data, but to also impose their own governance and risk management. Some organisations are establishing a data scientist's office, creating a horizontal data leadership function. This will create another CxO that IT functions will be required to align with.

Arrival of the CDO

Chief digital officer (CDO) positions have started to emerge in some industries, notably financial services and telecommunications. Just under 30 per cent of the respondents to IDC's CXO Survey 2017 now have a CDO responsible for driving the digital leadership team. As organisations progress up the digital maturity curve and look to scale their digital business by developing digital platforms that cut across traditional department silos, and launch an increasing number of digital services, the need to have an office focused on digital becomes apparent. In some instances, CIOs have assumed this role or added it to their responsibilities; in others, the two positons are kept separate and distinct. An independent CDO will certainly take away most of the digital transformation leadership responsibilities from the CIO and other CxOs. This will also create the need for a potentially complicated LoB-Digital-IT alignment.

IT for Digital at Scale

The next stage of digital development for many organisations, particularly in the telecommunications, financial services, and citizen-oriented public services areas, is to establish platforms that not only aggregate and integrate digital services for their customers, but also allow them to provide hyper-personalised digital services at scale. Such initiatives to scale digital business will likely be top-down driven, and probably led or largely influenced by the CDO and LoBs. As many businesses become mostly or entirely digital businesses, the influence and control that IT currently exercises over digital initiatives will decline.

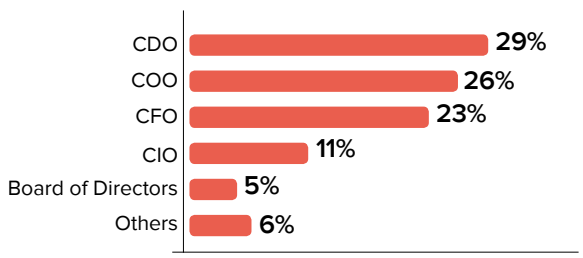
However, the IT function will be required to provide an agile IT-as-a-service platform for the business that enables digital to scale. These initiatives often require the integration of digital services of ecosystem partners and the alignment of their IT systems with that of the organisation. Eventually, much of the enterprise IT infrastructure will move to the cloud, and this will transform the role of IT into that of a service provider to LoBs, offering pay-as-you-go IT service, based on services level agreements (SLAs). This will lead to a fundamental redistribution of digital and technology responsibilities and budgets among the LoBs and IT functions.

A New Vision for the IT Function

As business transforms into digital business and innovation accelerates at the business end, the IT function will have the opportunity to contribute to this innovation but, perhaps more importantly, it will be under pressure to provide an infrastructure that is agile and secure to support this innovation, and integrate the innovation into the current IT environment. No doubt, digital transformation will lead to a significant redrawing of the lines of engagement between IT functions and CxO/LoB departments.

In this context, for the future, it is important for the IT function to articulate a new vision for itself – one that re-imagines it as an IT services business that generates revenue and profit from internal customers and eventually from external ecosystem partners as well. Some organisations may establish an internal open market where the IT function competes with external IT providers to acquire business from LoBs. This will create a new identity for the IT function, reshape the relationships with the LoBs, and furthermore, strengthen its relevance and contribution to the business.

Who drives the digital leadership team?



SOURCE: IDC CXO ME STUDY,, 2017

USING CLOUD TO IMPROVE RESILIENCY

Organisations constantly talk about securing their cloud environments. They don't realise they can use cloud to enhance their security, build resilient networks, and remain agile. IDC spoke to **Hans Nipshagen,** regional manager for web and security at Akamai Technologies, to find out more.

IDC: What is your view of cloud adoption in the region, and how is it changing the way organisations operate?

HN: According to IDC's own forecasts, worldwide spending on public cloud services will double by 2019 – almost six times the overall IT spending growth rate expected over the same period. This phenomenal growth is increasingly being witnessed here in the Middle East, where we are also seeing the wider adoption of cloud technologies. Companies and government agencies across the region are mirroring global cloud trends, with more of their daily activities now taking place outside of the traditional office.

They are increasingly engaging with customers and collaborating with coworkers over the internet, performing financial transactions, transmitting sensitive business data, and communicating over public networks. To do this, they are moving more of their applications onto internet-facing networks, so customers can shop 24/7 and employees can access the resources they need at any time in the global work day.

IDC: How important is it to address DNS security when it comes to cloud environments?

HN: DNS infrastructure security plays a critical role in the internet. It is, however, an often-neglected system and one that tends not to be addressed adequately from a performance and security perspective when designing and building an online presence. The attacks on DNS provider Dyn in October 2016 highlight the appeal of DNS servers as a target for attackers attempting to disrupt web operations. Even if the primary web target is well protected, attackers often target the supporting DNS infrastructure to prevent users from reaching the site. It is therefore important to have cloud protection in place to avoid DNS downtime.

IDC: An inevitable outcome of digital transformation is that it will lead to more open ecosystems. How do you expect this to shape the threat landscape over the coming years?

HN: Because of the more open ecosystem, attackers can more easily access a larger number of high-value corporate and government assets. Attackers have shifted their methods accordingly, developing new attacks that no longer rely purely on brute force to take a service offline, but rather probe for and then take advantage of application vulnerabilities to steal data or pursue financial gain.

The threat landscape is constantly evolving, and organisations must evolve to keep pace with the constant stream of new attacks. However, the increasing pace of change in the last few years requires a revolutionary, not an evolutionary, approach to security.

IDC: How should organisations address security in this new era, and how can they make sure they choose the right solutions?

HN: When comparing different approaches, organisations should consider the strengths and weaknesses of each solution – not just how they performs against the attacks of today, but also how well they will respond to those of tomorrow. Beyond the traditional metrics of scale and performance, architecture and adaptability will help determine the efficacy of any security solution over the long term. How well will the platform's architecture lend itself to defending against new attacks that haven't yet been discovered? And how quickly will it detect and identify those new attacks before it can mitigate them?

For organisations operating online today, finding the right partner means more than just protecting IT assets. The right partner can complement each organisation's online strategy with the right blend of security and performance. And the right partner can help organisations operate online with less risk, while taking advantage of the medium to offer a better internet experience for its users.

IDC: How is the threat landscape evolving, and what challenges does this present?

HN: For as long as organisations have operated online, attackers have looked for ways to target them. And as the internet has evolved, the methods and techniques used have changed to take advantage of the vulnerabilities that arise. The challenge with web security lies in that changing nature; attackers are always one step ahead of IT, constantly increasing the scale of attacks through massive botnets or looking for new ways to take down web applications and infrastructure.

The Panix attack in 1996 first highlighted the security threats that organisations face online. However, the threat landscape has changed dramatically since then. Starting at the network layer and moving to applications, the range of possible attack vectors continues to expand with no end in sight. With this shift, legacy security solutions are no longer as effective, while on-premises hardware and ISP-based DDoS mitigation services can lack sufficient scale and performance to protect internet-facing application infrastructures as they continue to grow.

IDC: So what should enterprises do to ensure a more responsive and secure environment?

As organisations move more of their operations online, they need a global cloud-based security solution that can defend their websites and other internet-facing applications, safeguard business and customer data, and protect their brand image from harm.

Not only can a global platform that is inline and always on provide the scale and performance to protect organisations' internet-facing presence today, but it can also offer the flexibility to respond to new attacks as they emerge in the future.

IDC: What do you see as the major challenge when it comes to securing all the different elements that make up today's enterprise environment?

HN: Websites and other internet-facing applications depend on a variety of infrastructure elements to function. These include the physical servers on which they run, the network infrastructure through which they communicate, and even the DNS infrastructure that directs client systems to the application.

Protecting applications from downtime and data theft requires all of these supporting elements to be protected from potential attack – a task that has become increasingly challenging as the IT landscape has shifted. Globalisation and the resulting distribution of IT assets around the world, the adoption of cloud services and infrastructure, and the increasing reliance on the internet for business operations have all contributed to a diffusion of the traditional IT perimeter.

IDC: Given the optimisation of budgets and the use of cloud to supplement on-premises systems, how does Akamai address securing such an environment?

HN: Akamai architected the Akamai Intelligent Platform as a distributed cloud platform to help organisations better protect their new, smaller, and more diffused perimeters wherever their IT assets are deployed and data is stored. The Akamai Intelligent Platform comprises multiple different technologies and networks that protect different parts of the application infrastructure.

For websites and applications, Akamai draws on over 230,000 servers deployed in over 130 countries and more than 1,600 networks, meaning our server platform extends from the website or application to within one network hop from 90 per cent of all web users. This provides Akamai with the global reach to manage bots and web scapers and to detect and stop both DDoS and web application attacks at the edge of the network, closest to where they begin and before they reach their target.

For origin infrastructure and non-web applications, Akamai has seven high-capacity scrubbing centers located around the world, meaning our purpose-built Prolexic DDoS mitigation network provides the capability to protect the entire origin infrastructure from DDoS attacks. It employs over 20 different security technologies to detect, identify, and mitigate any type of DDoS attack targeting either the infrastructure or any type of internet-facing application.

Finally, Akamai's independent DNS platform has been architected to ensure both performance and availability. It includes thousands of name servers deployed in over 200 points of presence around the world to improve DNS performance and provide the capacity to absorb the largest DNS-based DDoS attacks.

UNDERSTANDING AND ADDRESSING DDOS ATTACKS TO REMAIN RESILIENT IN THE DIGITAL ERA

An Akamai-sponsored Study by IDC

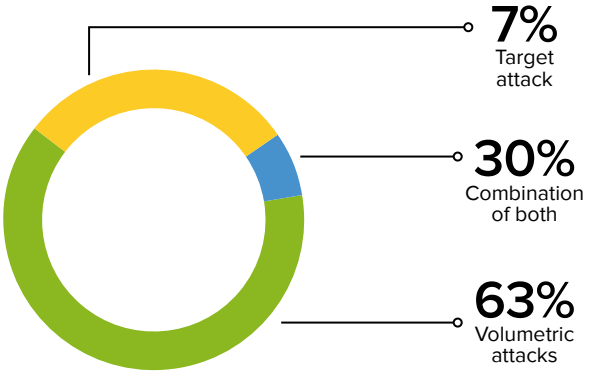
With digital transformation on the horizon, organisations in the Gulf have been adopting solutions such as cloud, mobility, and big data/analytics to sustain a competitive edge, modernise business processes, and meet the growing demands of customers and employees alike. The need for agile and responsive service delivery has been heightened by increased investments into mobile devices and applications, as well as the deployment of internet-of-things (IoT) technologies. This requires organisations to ensure that they can provide their customers (i.e., consumers and businesses) with the right level of experience and quality of service.

Higher levels of interaction and engagement with organisations across various networks are leading to far more open and dynamic ecosystems, many of which may fall outside the control of any single organisation or entity. Maintaining a secure environment is a major challenge: The adoption of new technologies and devices creates many new endpoints, all of which need to be secured. In the digital era, organisations and consumers are vulnerable to security incidents, which can be triggered by anything from a standard virus infection to hackers taking control of connected home appliances. Security will thus play a critical role in ensuring success for any organisation as it enters the digital era. Downtime due to a security incident can have severe implications for an organisation from financial, legal, and branding perspectives.

To this end, Akamai Technologies commissioned IDC to research the security landscape in the Gulf region and the impact of distributed-denial-of-services (DDoS) attacks. DDoS attacks use a botnet (a network of internet-connected computers infected with malware and controlled as a group) and DNS queries or other means to forward malicious communications to other computers on a network. When the website or network shuts down due to a flood of incoming messages, service is denied. In late 2016, many websites experienced downtime or became slow due to an attack on internet company Dyn, affecting users across numerous countries. Hackers were suspected of using millions of malware-infected devices connected to the internet to create the "botnet" needed to execute the attack, which, in turn, brought to light the vulnerabilities of the "world of things." DDoS incidents have impacted the websites and service levels of government, telecommunications, media, and finance organisations in the Gulf. DDoS attacks are increasingly being used as a method of extortion or as smokescreens for data theft.

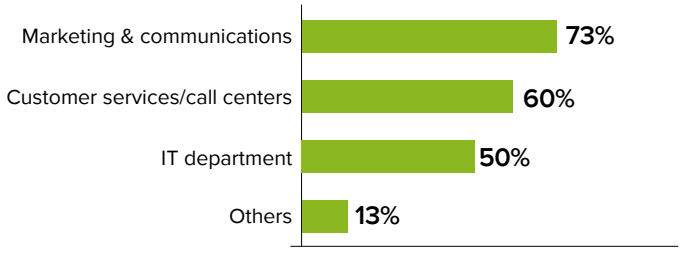
Many of the surveyed organisations had experienced DDoS attacks over the past 12 months. Nearly 63 per cent of those attacks were volumetric attacks; 7 per cent were targeted attacks; and the remaining 30 per cent were a combination of both. Volumetric attacks are the

Types of DDoS attacks experienced by organisations in the UAE & Qatar, 2016



SOURCE: IDC/AKAMAI, 2016

Departments impacted by DDoS attacks



SOURCE: IDC, 2016, N=30- ORGANISATION EXPERIENCED DDOS ATTACKS

most common DDoS attacks, with multiple infected systems used to flood a network and impact its services. Such attacks are hard to combat, since several systems are used in their execution. DDoS attacks lead to service disruptions and downtime, with nearly 50 per cent of the organisations surveyed indicating that they were offline for 6–8 hours because of such attacks. In 2016, marketing and communications departments were impacted the most by DDoS incidents, followed by customer service and call centers. As a result of such an attack, the brand reputation of the targeted organisation suffers and customers' ability to interact with personnel is curtailed. Service downtime essentially frustrates customers, negatively impacting customer loyalty and lowering brand/service expectations.

DDoS attacks are increasing in sophistication and becoming more pervasive and persistent than ever before. This makes it critical for organisations to plan and deploy solutions that facilitate effective detection and mitigation so that they can remain resilient in the digital era. Knowledge of DDoS attacks (as well as broader security awareness) is critical for business leaders. Many such attacks (in both the region and elsewhere around the world) are, ultimately, the result of a lack of user awareness or due to basic errors within systems and programmes.

To build an effective DDoS mitigation strategy, organisations must understand their network traffic so that they can detect anomalies and malicious behavior. Leveraging knowledge of the entire network, such as the reputation of the DNS, domain names, and registration details, will enable IT to preempt concerns about traffic flow. In addition, organisations in an open ecosystem need to be more aware of the threat landscape, both regionally and globally, so they can better evaluate the potential impacts on their networks. With constraints around budgets and skills, organisations can leverage the services of ISPs — or even security services providers — to help them remain up to date in terms of the latest threat intelligence. Many ISPs and security services providers also provide DDoS mitigation services. Organisations could also consider a cloud-based solution, or "DDoS mitigation as a service," as it may take away the pressure of managing such a solution internally. Furthermore, cloud-based solutions enhance protection by being closer to the source of the attack, and they provide a strong abstraction layer for corporate enterprise resources. Lastly, bear in mind that many DDoS attacks are used as smokescreens for other critical security breaches. Immediately after a DDoS attack, organisations must evaluate whether any data breaches or other security incidents have occurred or are occurring. A high degree of automation will help organisations in the critical early detection and mitigation phases.

DIGITAL TRANSFORMATION WILL BECOME THE NEW NORMAL FOR GULF BUSINESSES

By **Jon Tullet** – Research Manager, IT Services – IDC Middle East, Turkey and Africa

Digital transformation is well underway across the Middle East, as it is worldwide. CIOs surveyed by IDC indicated that only 16 per cent of businesses in the Middle East had no plans at all to conduct formal digital transformation (DX) programs *(IDC Middle East CIO Survey, 2016)*. These extend far beyond technology updates: IDC defines digital transformation as a continuous process by which enterprises adapt to or drive disruptive changes in their customers and marketplaces, by leveraging digital competencies to create new business models, products, and services.

This trend is driving IT out of the back office and into the forefront of boardroom strategies. From a business support role, the IT operation is maturing to become an instrument of business agility, efficiency, and cost optimisation.

Agility and cost optimisation are the hallmarks of cloud solutions; these are the key advantages espoused by public cloud vendors, promising the ability to deploy complex solutions quickly, with customers paying only for the resources they consume. Cloud adoption across the Middle East is gathering momentum, with 46 per cent of CIOs indicating that they will have applications deployed in the cloud by 2017, as businesses look to improve their agility and shift big capital expenditure (CAPEX) outlays to ongoing operating expenditure (OPEX) budgets.

However, while IDC remains confident that most enterprise workloads will, ultimately, migrate to cloud infrastructure, in the near term it is almost inevitable that most organisations will embrace a hybrid IT strategy. Very few organisations have the capability or desire to move their entire technology stack to the public cloud, nor does it make business sense to do so. A better approach is a gradual transition, moving workloads and applications as it makes sense, resulting in a hybrid mix of public cloud services and on-premises solutions; the latter should, by now, be making extensive use of cloud technologies and practices anyway.

This hybrid approach reflects a transformation, to a model of applying a best-case deployment for each application; by its very nature, that implies business benefit. The key to future success is to ensure that whatever model is

adopted is also flexible enough to continue that transformation as the environment changes. Workloads should be able to move into or out of the cloud with minimal disruption, or indeed take advantage of moving a subset of functions between locations.

One example of this in practice is in extending the capabilities of enterprise resource planning (ERP) solutions. Many organisations today use ERP applications to manage their key processes. Regardless of whether these applications are on premises or in the cloud, organisations can benefit from the ability to add additional capabilities quickly and seamlessly, through cloud platforms. Emerging technologies such as machine learning can be brought to bear by, for example, providing analytics and forecasting to optimise supply chains, logistics, and inventory management. By taking this hybrid approach, significant business benefits can be achieved without a complex upgrade of the existing infrastructure.

For software vendors, this approach is optimal because it allows their customers to quickly test a solution, deploy it, and measure business impact, greatly reducing organisational friction and risk. This approach also encourages local providers to proffer niche solutions alongside the monolithic, and usually international, solutions dominating the enterprise application marketplace.

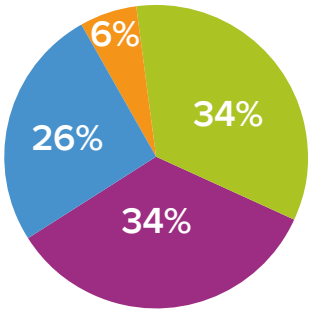
This is, of course, not limited to ERP applications; similar ecosystems are springing up in other areas such as customer relationship management, infrastructure management, security, and many more. IDC has described an "innovation ecosystem" developing on top of the third platform (the combination of cloud, big data analytics, mobile, and social applications). Emerging technologies such as the Internet of Things and machine learning are becoming readily accessible, deployed in and through cloud services, enabling next-generation services to develop without costly and disruptive infrastructure rip-and-replace exercises.

One of the interesting side effects of this transformation is the shift in boardroom dynamics. The CIO is becoming more involved in business strategy, while other C-level executives, particularly the chief financial and marketing officers (CFO and CMO), are becoming more closely involved in technology decision-making. Across the Middle East, CIOs rate the CFO as one of the top three executives to be involved in the digital transformation process (the other two being the CIO and the CEO), with the CMO closely behind. There is clear recognition that financial management and business oversight are critical inputs to a digital transformation process which encompasses far more than just technology.

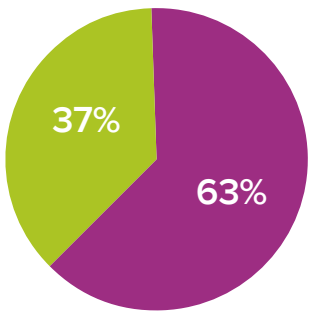
This change also creates an opportunity to bring a serious business risk under control: shadow IT. This occurs when line-of-business managers, or even employees, initiate IT projects without proper oversight. Cloud services are particularly common, as they can be easily provisioned directly by end users. Aside from security risks, this can also create an OPEX time bomb; shadow IT costs tend to mount in the background, with little transparency until they are out of control. There is also the opportunity cost incurred by the lack of coordination and integration between isolated projects, or lost productivity when a side project is abandoned. The digital transformation process allows the IT department to evolve from a strict gatekeeper of permitted services, to a facilitator whose role is to educate and to empower such projects, while ensuring governance is maintained.

Digital transformation is gathering pace in the Gulf, and is likely to become the new normal for competitive businesses. IDC expects deployment of cloud solutions to continue to accelerate under hybrid IT strategies designed to maximise efficiency and business benefit, ultimately leading to new business practices and products. This hyper-competitive landscape will also pose severe challenges for organisations that fail to transform in the face of disruptive market change.

Current state of DX adoption in the Middle East



Current usage of cloud in the Middle East



SOURCE: IDC CXO ME SURVEY, 2017 N= 151, RESPONDENTS USING CLOUD COMPUTING WITHIN THEIR ORGANIZATION

AN INTEGRATED STRATEGY FOR SECURING THE CLOUD

Cloud is not limited to applications alone; it is the infrastructure of the future. Organisations should prioritise security on the cloud as much as they do their on-premise environment. **Ronen Shpirer**, Senior Manager, Solutions Marketing at Fortinet, shares his views on cloud and how organisations can address cloud security.

IDC: In your experience, do you find that organisations take a more proactive approach to security when it involves cloud?

RS: There are two somewhat conflicting forces at play when it comes to enterprises securing their cloud environments – the fact that it is relatively easy to do and the fact that many organisations don't appreciate the need to actually do it!

As clouds may exist within enterprises' own datacenters (ie, private cloud) and those datacenters are secured by perimeter and core firewalls along with application-level security appliances, some organisations can fall into the trap of thinking that their private cloud is also secured by the same security infrastructure.

However, this is not the case. While it is certainly required, the existing physical datacenter security infrastructure is not enough, so it is imperative that a virtual security infrastructure is implemented within the private cloud itself.

IDC: And what about public clouds? Do some organisations overly rely on the cloud providers to secure their data?

RS: Absolutely. When it comes to public clouds or hybrid environments (ie, combinations of private and public clouds),

enterprises sometimes fail to understand that they also have a part to play in securing their assets that reside in those clouds. Indeed, there should never be an assumption that this will be taken care of by the cloud provider.

The irony is that implementing security in a cloud environment, and particularly in a public cloud environment, is relatively straight forward. It does not require capital investments as pay-per-use business models are widely available with all the major cloud providers.

So, in theory, securing an enterprise's public cloud environment is a simple task – as long as the enterprise understands that it has a responsibility to do so. Essentially, it is the level of this awareness that determines how proactive the enterprise will be in securing its cloud environments.

IDC: How have you been supporting customers in securing their private cloud deployments?

RS: At Fortinet we have a wide range of virtual security appliances for both private and public clouds. Furthermore, our solutions integrate with our customers' underlying cloud automation and orchestration systems so that the appropriate security is deployed and provided where and when needed – all in an automated fashion. We have been supporting thousands of enterprises in securing their private and hybrid cloud environments – VMware ESXi and NSX, Microsoft Hyper-V and Azure, OpenStack, AWS, and more.

IDC: With lots of organisations now consolidating their datacenter investments, how would you advise they address security within next-generation datacenters?

RS: The first step should be to implement perimeter and core datacenter security to protect the datacenter and perform internal security segmentation. All of this must be done for a high amount of data, running on high-speed Ethernet, without slowing down applications and hurting the user experience. To do that physical, ASIC-based security appliances are required. And with cloud widely used, a second layer of security based on virtual security appliances must also be put in place. This will help to secure the virtual environment as well, ie, the cloud (both private and public).

IDC: And the approaches to physical and virtual security should be coordinated?

RS: Yes. It's important that both the physical and virtual security infrastructure use a common set of threat intelligence and security policies. This will help to ensure an end-to-end security posture and avoid any potential security gaps between the physical and cloud environments.

It should also be noted that in order to effectively identify areas of weakness and potential gaps, security operations (management, reporting, SIEM, etc.) must be provided end to end. Ensuring end-to-end network and security visibility allows for better event correlation and the acceleration of mitigation once a breach has been detected.

IDC: Given that security is considered critical for enabling effective digital transformation, what should customers keep top of mind?

RS: Security is indeed a fundamental part of digital transformation, serving as both an enabler and a foundation for the process. Digital transformation will not be able to provide its full benefits if it does not have security as one of its foundations. Therefore, security considerations, strategy, and planning must form an integral part of the ongoing change that is digital transformation.

IDC: And all of this must be integrated across the entire network in order to be truly effective?

RS: Exactly. The role of the network in any business strategy is now more important than ever, and ensuring it's both fast and secure is critical to enabling success. Having an effective security strategy for your entire network can determine whether you are running a smooth, safe organisation or about to become the latest security breach headline.

While cyberthreats are becoming more powerful, networks are becoming more disjointed and complex. To enable an effective defense, the data and security elements across all the organisation's various environments must be well integrated, able to share intelligence, and visibility.

IDC: How can Fortinet help in this regard?

The Fortinet Security Fabric is our technology vision. It is an intelligent framework designed to deliver scalable, integrated and collaborative security combined with high awareness, actionable threat intelligence, and open APIs. It drives our products and solutions development in such a way that it gives customers control, integration, and easy management of security across the entire organisation, from IoT to the cloud. It also closes any gaps that were most likely introduced when disparate security products were added, datacenters migrated, and/or networks expanded.

IDC: And how exactly does it do this?

The Fortinet Security Fabric has three key attributes: Firstly, it is broad; this enables it to cover the entire attack surface, meaning security can be applied to the network, endpoints, access, applications, and cloud. Secondly, it is powerful; it uses security processors to reduce the burden on infrastructure, delivering comprehensive security without affecting performance. And thirdly, it is automated; this enables a fast and coordinated response to threats, with all elements able to rapidly exchange threat intelligence and coordinate actions.

Ultimately, the Fortinet Security Fabric allows security to dynamically expand and adapt as more and more workloads and data are added, and at the same time, seamlessly follow and protect data, users, and applications as they move back and forth between IoT, smart devices, and cloud environments throughout the network.

FORTINET

BUILDING A CLOUD STRATEGY THAT WORKS FOR THE BUSINESS

By **Megha Kumar** – Research Director, Software and Cloud – IDC Middle East, Turkey & Africa

There is no denying that digital transformation is a reality that we all need to comprehend, and one which creates synergies between IT and business. Based on a survey conducted by IDC in 2017, business leaders in the Gulf region believe that digital transformation is critical for them to remain competitive and relevant.

This need to remain relevant has a lot to do with the changing demographics in the region and the disruption being created by companies such as Uber, Careem, and Airbnb, as well as by various fintech firms (IT vendors to the financial services industry). The region has the largest youth population in the world, with young people interconnected with one another and using multiple devices. This puts pressure on businesses to be accessible anytime, anywhere, and on any device.

Business decision makers are under the same pressure as IT to optimise budgets, standardise processes, and achieve greater efficiency. IDC believes that the use of 3rd Platform technologies (cloud, mobile, social, and big data), alongside technologies that are accelerating innovation, such as the Internet of Things (IoT), cognitive systems, and virtual/augmented reality, will enable businesses to realise their priorities and digital transformation ambitions. We also believe that cloud will underpin much of the infrastructure in the region in the future. In addition to providing access to compute and storage capacity on demand, cloud has made it easy for organisations to gain access to the latest business applications.

Cloud technologies will play a central role in enabling organisations to achieve their omni-channel ambitions, and will also ensure the successful use of big data technologies. Cloud will provision access to applications and systems anytime and anywhere. The use of cloud can help complement compute and storage capacity for big data projects if needed, and will also support IoT deployments.

IT decision makers have always believed that cloud adoption is essential, largely due to cost savings, the ability to scale, and the capacity to provision services faster than ever before. This contrasts with business decision makers who believe that the main reasons for cloud adoption are faster access to advanced

workloads, better service, value, and security.

Financial decision makers stated that their reasons for using cloud are largely due to the belief that it offers better value in terms of services and allows for better security and faster deployment. Security has traditionally been a major inhibitor when it comes to cloud adoption. Financial decision makers believe that cloud provides better security, highlighting the fact that cloud services providers invest heavily in data and datacenter security. For marketing decision makers, the value is largely based on access to advanced workloads, the flexibility provided by cloud, improved security, and mobility. Marketers in the region are focused on improving their omni-channel presence, and cloud will allow for the provisioning of touchpoints across various devices and applications. These capabilities were highlighted as the main reason for cloud adoption by business decision makers.

As stated above, digital transformation initiatives require business divisions to view technology as the core business, rather than solely as an enabler and leaving it in the hands of IT. It is becoming increasingly clear that business and IT can no longer be siloed. In terms of driving cloud adoption, we have highlighted a few aspects that business decision makers should consider moving forward:

• Adopt a cloud-first approach: Many of the functionalities that need to be accessed by marketing and finance are available as a service. Work with IT to evaluate whether your current enterprise software provider has these workloads available as a service. Alternatively, look at the best provider in the market and evaluate whether their solutions

fit within your budget and can be integrated with existing systems.

• Work with IT: This is crucial because internal IT can help ensure that cloud solutions are integrated properly and comply with the standards set within the organisation or by the industry itself. Streamlining processes will help optimise costs, while compliance will also help to avoid any adverse financial or legal repercussions.

• Security is your problem: It is easy to brush off security and make it IT's concern, but this cannot be the case. As a department leader, you will need to work with IT to define what is critical for your division, what can or cannot be accessed by employees, and ensure that the systems are up to date and secure. This should be the attitude toward both on-premises and cloud systems. You will also need to work with IT and HR to build out end-user security awareness. A security breach can damage a brand and lead to financial penalties.

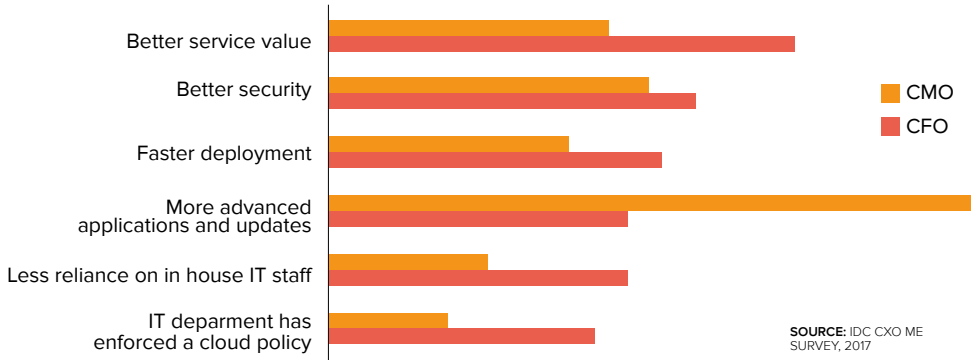
• Define your service-level agreements (SLAs): Work with IT and legal personnel to build out the SLAs for your department with your cloud services providers in terms of updates, support, migration, and portability. Understanding cloud metrics will be useful for understanding the cost of utilising cloud technologies and the recurring operational expenses that will be borne by the department.

• Get your team involved: Cloud solutions (or any solutions for that matter) only represent a reasonable investment if the user experience is seamless. It is good to get team input regarding the functionalities and to formulate a change management plan. Such steps will be essential in preventing a potential drop in service levels and productivity.

• Shadow IT: While you can procure your own IT solutions as a business decision maker, IDC suggests involving rather than ignoring the IT department. Solutions need to be secure, and procuring a solution without IT involvement can lead to security and compliance concerns.

These are a few of the aspects that business decision makers should consider. Also, keep in mind that your industry is changing, and the pressure to sustain agility and competitiveness is more vital than ever before. Leverage best practices from your peers and the overall region. Digital transformation will require a certain level of risk propensity, and will be critical to remain relevant.

Top 5 reasons for using cloud



SOURCE: IDC CXO ME SURVEY, 2017

HOW CAN LINE-OF-BUSINESS EXECUTIVES SUPPORT SAUDI ARABIA'S NATIONAL TRANSFORMATION PROGRAM?

By **Hamza Naqshbandi** – Principal Analyst – IDC Saudi Arabia

Saudi Arabia's oil wealth has enabled the kingdom to undergo unprecedented modernisation, including widespread infrastructure development and a strengthening of the business environment. However, diversifying away from an oil-based economy has undoubtedly been a challenge. Indeed, the sharp decline of global oil prices has led to a significant revenue shortfall that has had a ripple effect across all walks of life in the kingdom.

In 2016, the government announced a plan to combat this. Called 'Vision 2030', this comprehensive plan comprises regulatory, budget, and policy changes that will be implemented over the next 15 years with the aim of building a "prosperous and sustainable economic future" for the kingdom and making it much less reliant on crude oil.

The Vision 2030 blueprint outlines a number of major executive programs. And chief among them is the National Transformation Program (NTP), which provides relevant government entities with a detailed roadmap – including regional and global benchmarks, performance indicators, and expected outcomes – for achieving the goals set out by Vision 2030.

The Saudi Arabian ICT market is the largest in the Middle East, and while IDC has observed a significant slowdown in hardware spending in the kingdom, spending on enterprise software and IT services continues to grow. The government has been emphasising the importance of technology as part of its strategic plans in recent years, and this has seen ICT investment become a top priority.

Unsurprisingly, then, digital transformation (DX) will play a pivotal role during the entire lifecycle of the NTP, as Saudi enterprises look to transform themselves into more agile, flexible, and customer-centric organisations. There will also be a sharp focus on improving management decisions and accelerating the development of new products and services.

Much has been made of the ongoing digital revolution, which typically refers to the widespread adoption of smart and connected ICT by consumers, businesses, and governments. And as this trend gathers momentum in Saudi Arabia, there is no question that digital technologies will have a considerable role to play in improving the kingdom's economic performance, societal wellbeing, and overall governance.

The last edition of IDC's annual Saudi Arabia CIO Survey conducted in 2016 showed that almost 90 per cent of respondents had either started their DX initiatives or were planning to get them underway. And since digital transformation is a multifaceted process involving not just the transformation of the IT function but of the entire organisation, a unified team effort across all departments is required. This means that the role of line-of-business (LoB) executives is critical to ensuring a smooth and successful DX process (see Figures 1 & 2).

LoBs do not just have a role to play in influencing ICT procurement; their involvement encompasses the overall utilisation of emerging technologies with the aim of driving business growth.

And as NTP-related initiatives move from the strategy phase to implementation, the influence of emerging technologies on driving the business forward will become even more stark, necessitating an unprecedented level of collaboration between all stakeholders (IT, business, and management).

While CIOs are tasked with enabling a slew of transformational projects across the organisation, they are increasingly grappling with shoe-string budgets and a shortage of advanced IT skills within their teams. As such, the pressure of digital transformation is affecting the office of the CFO, with the age-old need to balance the books rapidly expanding to encompass the more strategic role of data-driven decision-making.

Similarly, CMOs are increasingly seeking cost-effective social technologies and enterprise mobility solutions to target new customers while simultaneously streamlining their operations and costs. Shadow IT is no longer a well-kept secret, and as NTP initiatives gather momentum, the impact of shadow IT will need to be curtailed and inefficiencies around IT procurement timelines and processes will need to be addressed.

Business funding will be vital to enabling transformational initiatives, and Saudi IT leaders will need to better understand business requirements and propose relevant solutions that help in meeting business imperatives, while balancing the compliance and security dimensions.

While it is evident that technology cannot replace oil, it is hard to ignore that it is fast becoming an indispensable enabler in disrupting the traditional frameworks of all walks of society in Saudi Arabia. The NTP, with its mandate to drive unprecedented change, will embrace all the benefits that digital transformation brings to the table and, in many ways, will shape the kingdom's digital future.

The NTP will necessitate Saudi business leaders to constantly challenge their organisations to ensure this transformative phase will unlock productivity gains and significant competitive advantage, all while delivering exceptional customer experience. IT needs to be prepared to play its part in this journey, both as a facilitator and as a trusted implementation partner.

To read more on the ICT led approach to the National Transformation Plan go to www.idcntpreport.com.

Q: As CIO, which best describes the focus of your role as it relates to your organisation's digital transformation efforts?

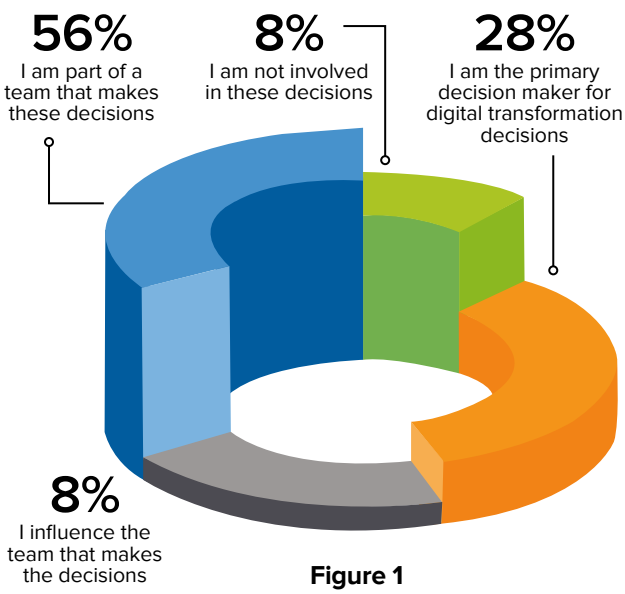


Figure 1

Q. How would you describe your organisation's digital transformation efforts?

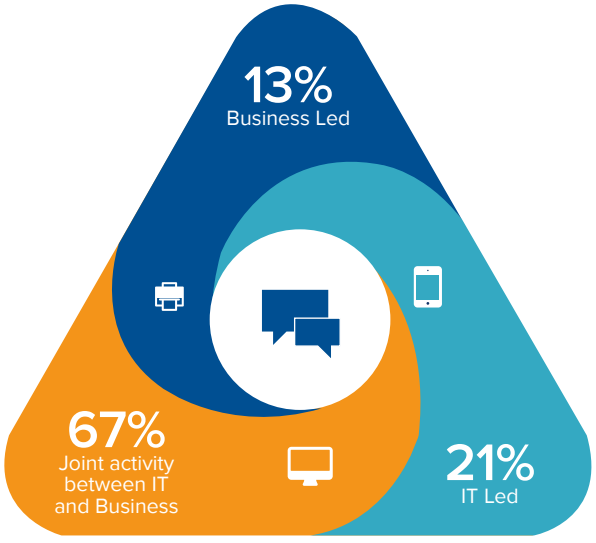


Figure 2

SOURCE: IDC KSA CIO SUMMIT, 2016

Find your place in the NEW DIGITAL ECONOMY

In the world of digital transformation, there are resisters, explorers, players, transformers, and disruptors.

Where is your business?

- If you have not already developed a digitally enhanced, customer-focused strategy, *now is the time to begin.*
- If you are taking a case-by-case approach to building your digital initiatives, *now is the time to advance.*
- If you are struggling to scale your digital initiatives across your organization, *now is the time to move forward.*

If you think digital transformation is a hard process to tackle, think again. IDC is leading the way in advisory services for digital transformation and we are ready to help you now.

IDC
Analyze the Future

www.idc-cema.com