WHITE PAPER

A digital transformation blueprint for enterprises in Asia Pacific

LUMEN
The Platform for Amazing Things

Digital transformation in APAC

Over the past years, hybrid working has become permanent for most enterprises bringing networking, connectivity, and security challenges with the existing infrastructure to the fore. Asia Pacific (APAC) enterprises take advantage of new opportunities in emerging technology to digitise and digitalise their business model.

The motivation for digital transformation is not only influenced by changes in the workforce and business, but also driven by changing consumer behaviour and an increasingly competitive landscape. All these factors are forcing companies to accelerate their digital transformation plans — or at least to look for agile blueprints and roadmaps for digital transformation.

Indeed, most organisations today already make use of digital tools or infrastructure — whether it's ERP solutions or public cloud. However, having an array of disparate digital resources does not equate to digital transformation, although they might indeed benefit organisations by enhancing efficiency or reducing costs in the near term.

The digital transformation market size is projected to grow at a compound annual growth rate of 21.1%, from $594.5 billion in 2022 to $1,548.9 billion in 2027, according to Markets & Markets.

Digital investments create direct business value and are essential to achieving operational excellence to differentiate in a saturated market with signs of a global recession on the horizon. It is essential to keep the customer at the centre of all digital transformation strategies and create a blueprint for transformation with this in mind.

LUMEN

The four pillars of digital-first business

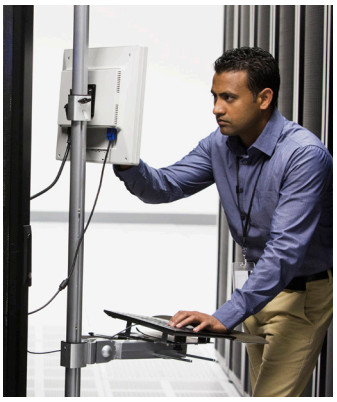
Generally, digital transformation is defined as employing technologies such as the cloud, big data, cybersecurity, automation, and so on to transform the way businesses operate. These are aspects of digital transformation, but do not define what digital transformation really is.

For an organisation to be truly digital-first, each aspect of the business should be digitalised in a structured manner, blending seamlessly into all other aspects of the business. Rather than digitalisation for its own sake, or merely increasing the efficiency or profitability of parts of the business, digital transformation should aim to future-proof an organisation and build resiliency.

A digital-first business should be underpinned by four key pillars:

- **Modernising IT**
- **Enabling digital experiences**
- **Digitalising operations**
- **Creating new business models**

LUMEN



Modernising IT

Many organisations today still rely on legacy systems that are inefficient, and sometimes also costly to maintain. These legacy systems, while having been useful in the past, are today becoming more of a hindrance than a help. They can drain resources, require too much maintenance, and often do not meet the standards of efficiency demanded by the users today.

Any successful digital transformation effort should aim to modernise the organisation's IT infrastructure and processes, whether it be re-architecting the infrastructure and operations or modernising the network and applications. Modernisation should address the following questions:

Does it improve the organisation's technology capabilities?

A modernised IT environment should be able to handle more workloads, support a diverse array of applications, and handle dynamic network traffic and access. It should also be agile and flexible enough to adapt to newer technologies. By 2025, 75% of enterprises will implement business models based on cloud (Gartner).

Does it increase the efficiency of operations and business processes?

Whether it's simplifying complex processes or streamlining operations, IT infrastructure must support the business functions. For example, network technologies such as SD-WAN and SASE can unify networking and security operations, whilst automation, artificial intelligence (AI) and machine learning (ML) can enable the execution of labourious tasks with greater speed and accuracy.

Does it increase employee satisfaction?

Employee satisfaction is key to retaining employees, boosting efficiency, and maintaining a positive workplace culture. IT modernisation today must be focused on improving the way employees work by making sure the infrastructure and applications are adaptable to new ways of working, such as BYOD and remote working.

LUMEN

Digitalising operations

Organisations today do not have a lack of option when it comes to solutions for digitalising their business. While most have moved on from manual spreadsheets and paper documents, many organisations fall into the trap of digitalising in silos, without keeping in mind of their digital-first goal.

This can result in the acquisition of Software-as-a-Service (SaaS) or cloud-based platforms that do not bring business value, or can't be integrated with other business functions or tools. Furthermore, this also exposes the organisation and its data to the evolving threat landscape. Digitalising operations should help organisations to:

Save time and resources

In this hypercompetitive global market, digitalisation should enable users to complete task quicker and at a lesser margin of error. Many organisation's innovation and growth plans now integrate AI, ML and emerging technologies to deploy solutions rapidly, securely and cost-effectively. It has been predicted that 40% of large enterprises will expand AI/ML usage across all business-critical horizontal functions (IDC).

Rationalise returns on investment

Ultimately, transforming business operations should bring increased returns on investment. Before investing in the latest technologies, organisations need to make sure they have an IT infrastructure that's adequate to handle growing workloads and apps, business processes that are integrated and efficient, and people with the right skill sets.

Boost productivity

Along with time savings, technology should encourage workplace productivity. This can come in many forms. For example, a digital automation platform can make employees more productive with their time and allowing greater focus on more strategic work.

4 in 5 global IT decision makers: Applications are a key differentiator for their service and customer interactions

Enabling digital experiences

Customer is at the centre of any business. Delivering consistently great customer experience makes it possible for organisations to reach a wider base of customers more frequently and improve brand loyalty. This is especially important for digital-native businesses, where a large part of their revenue comes through digital experiences.

To become a customer-centric organisation, digital experience is a top priority. 4 in 5 global IT decision makers say their applications are a key differentiator for their service and customer interactions, according to a research commissioned by Lumen.

However, without modern IT infrastructure and applications, it can be difficult to innovate at the speed of the market and keep consumers engaged.

Robust IT infrastructure

There are limitless ways for organisations to innovate and grow thanks to the emergence of new technologies. These are dependent on IT infrastructure designed to securely deliver and run applications and data. Organisations must modernise their network and cloud operations to handle the growing number of users, data volumes and application performance.

Securing customer data

Besides having the ability to handle growing data workloads, securing customer data is part of the digital experience as any breach can result in loss of trust and reputation. Consequently, mishandling of data or cyberattacks can severely impact the organisation's bottom line. According to KnowBe4, cybersecurity incidents cost organisations $1,197 per employee, per year.

Fast, connected, personalised experiences

Organisations are now customising customer experience based on preference, time, event, and location. To keep up with customer demands, they must be able to process data into actionable insights which means the IT systems cannot be an obstacle.

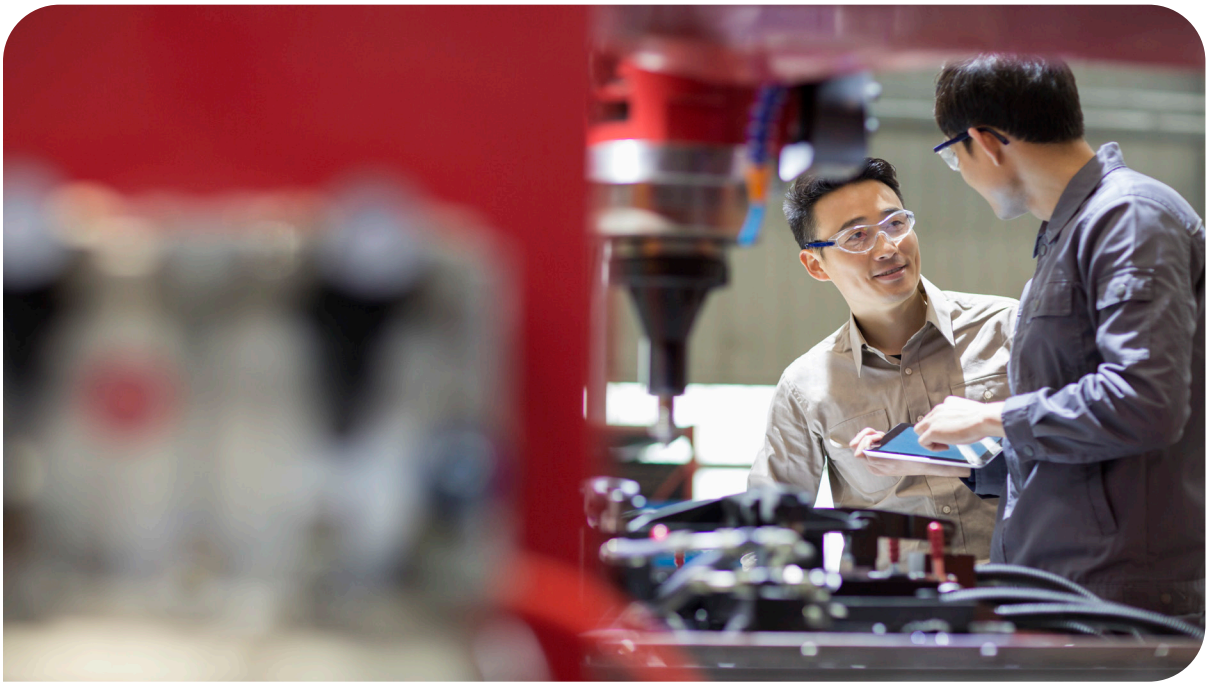
LUMEN

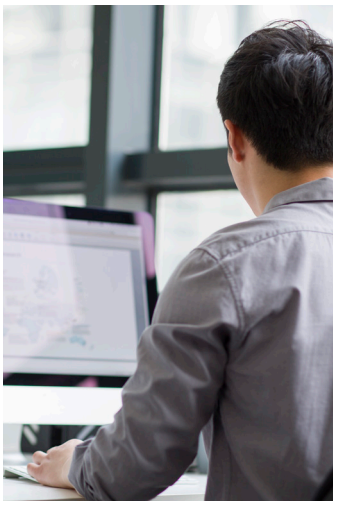
Creating new business models

With new digital technologies come new ways of doing business. In today's digital-first economy, traditional business models are increasingly threatened by agile, digital native competitors. Examples include Grab vs taxi companies, Netflix vs TV networks, Airbnb vs global hotel chains, and the list goes on.

Established organisations are now forced to compete with these new business models that promise customers faster, more efficient services. As such, digital transformation should ultimately aspire to keep businesses current and strengthen their competitiveness in this economy.

For example, in the banking sector, where incumbent banks are now facing competition from digital-only banks. In response, many of these banks have digitalised their business model to allow self-service banking on mobile apps for transacting, pay bills, and even for investing. However, as banks compete, they face new challenges in managing their IT infrastructure, data protection, and most critically, cybersecurity. A digital-first organisation, therefore, must also stay cognizant of the challenges that new technology brings.



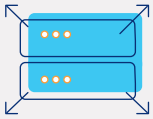


Taking the leap to become digital-first

Building a reliable and secure cloud environment

Almost all organisations today are on the cloud, even if it is something as simple as adopting cloud applications or storage. Indeed, many have migrated their servers partially or wholly to the cloud, and others are eager to make that transition.

For enterprises, the cloud has tremendous appeal for several very compelling reasons:



Elasticity, agility and scalability

The ability to scale up and down according to an organisation's immediate requirements is the main impetus behind cloud migration. Rather than paying high fixed costs for limited bandwidth and storage, as in the case of the traditional data centre, organisations can minimise cost while maximising capabilities.

Managed services

Cloud offers an array of managed services which eliminate the need for organisations to build and maintain their own hardware and software. This allows organisations to save time, space, and cost, as well as employ a leaner workforce that is geared towards other tasks.

Wider choice of cloud native apps

The past few years have seen a flowering of cloud-native applications, from collaborative software to development environments, which cannot be run on-premise. The cloud, therefore, offers organisations more options without the hassle of in-house development or storage issues.

LUMEN

Challenges of cloud migration

The cloud can seem so appealing that organisations eager to jump on board are oblivious to its difficulties. These are some of the challenges that organisations should be aware of:

Limited cost savings

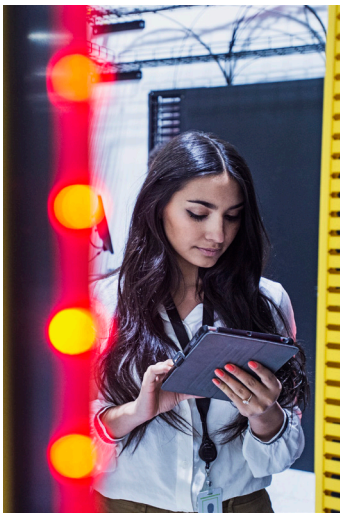
Many organisations are disappointed when they find the cost of the cloud equalling, or even exceeding, that of running their own on-premise data centres and servers. This is made worse by the fact that the cost of running operations in the cloud can be very unpredictable, given its scalable and agile nature. Planning and budgeting, therefore, can present a challenge and costs might end up being more than expected.

Usually, the main reason why the cloud ends up being more expensive than anticipated, is due to the approach organisations take when moving to the cloud.

Many organisations take a “lift and shift” approach, in which all their current applications are simply moved from on-premise servers to the cloud. This may present a problem because cloud servers are not identical to servers on on-premise data centres; applications that work well on-premise might not work well on the cloud.

A case in point are legacy Commercial Off-the-Shelf (COTS) applications, which often cannot work on the cloud. In fact, many large enterprises intending to move fully to the cloud have been forced to retain their data centres to host these applications.

Even discounting COTS, many other legacy applications require some tweaking before they can operate efficiently on the cloud. Therefore, a careful study of the compatibility of an organisation’s workloads is necessary prior to cloud migration.



Security and visibility

The cloud can be complex and requires new paradigms to ensure security and visibility, especially when an organisation is using a distributed network. Most APAC organisations believe they are most vulnerable to severe security breach regarding their cloud assets (13%) and network (14%).

Organisations choosing to run their own cloud servers independently should ensure they have the know-how to be able to continuously monitor their IT environment, in real-time, to prevent any compromises with security.

Fortunately, today, there are public cloud platforms that can provide organisations with these tools. Ideally, an organisation new to the cloud should select a partner who is able to handle security and visibility, in addition to giving the organisation over their cloud resources. Also not forgetting cloud security services that identifies, prioritises and remediates security risks and compliance issues across the entire cloud estate.

Most APAC organisations believe they are most vulnerable to severe security breach regarding thier cloud assets (13%) and network (14%)

Hybrid cloud and multi-cloud: Models of the future?

When switching to the cloud, there are a number of options open to organisations. The first option is usually between private and public cloud – that is, choosing between one's own data centre or servers, or a cloud provider's servers.

As the private cloud is usually more expensive but may also offer greater data security and flexibility, large enterprises wanting to balance cost and security have begun to adopt a hybrid cloud model. Here, workloads and applications are segregated according to their requirements, and placed in the private and public cloud depending on the type of data each contains. Some organisations will choose to combine the cloud with on-premise infrastructure, especially in industries holding highly sensitive data, such as in banking.

Another model organisations are turning towards is the multi-cloud, in which multiple public cloud providers are used by a single enterprise. This way, organisations can build a best-of-breed public cloud environment and benefit from each platform, such as cost savings and flexibility. To do this, an organisation needs to understand how each of its workloads operates, as well as other requirements such as the level of security needed, before migrating it to an appropriate platform.

READ CASE STUDY: RICOH

LUMEN

Dealing with the data quagmire

Large and medium enterprises are faced with the difficult tasks of storing, managing, and analysing large volumes of data to drive insights and achieve profitable business outcomes. How can organisations better understand and protect their data?

Data management checklist

To begin tackling this, enterprises must first be aware of the data lifecycle within the enterprise. The following checklist can serve as a quick guide for enterprises planning their data strategy:

1. What data is being collected?
2. Where is the data being collected from?
3. Where is the data being stored?
4. How is the data being processed?
5. How does the data flow throughout the organisation?
6. Who is responsible for each stage of the data flow?
7. Who uses this data on a day-to-day basis?
8. How long will the data be stored in the organisation?

1 in 3 global IT decision makers: Securing organisation's data is the most challenging task of their career

Data storage can go out of control

Even if organisations know exactly where their data is and what it is being used for, the overwhelming amount of data generated each day means an increased demand for storage – even if temporary. As the data grows and accumulates, enterprises must find more and better ways to keep up, or risk spending an inordinate amount of money and resources trying to find space for it.

One of the ways to do this is use a multi-cloud model, wherein different data sets are stored on different platforms depending on the requirements. However, this can both be very messy, especially if the data needs to be shifted from one platform to another, while posing security challenges.

Data security and privacy: A key challenge

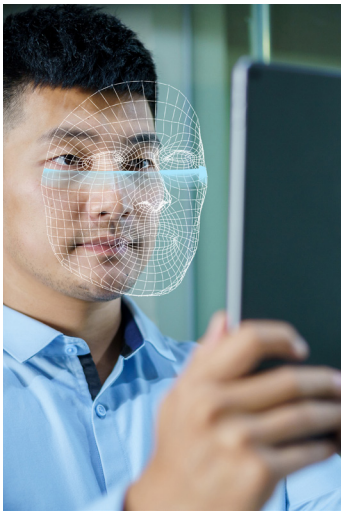
With stringent data protection laws in most countries around the world, one of the primary concerns for organisations is the challenge of data protection. Aside from the real and opportunity costs of stolen or leaked data, the business leaders may also face stiff regulatory penalties for improper data protection and, perhaps even more damaging, the risk of having its reputation tarnished. According to research commissioned by Lumen, 1 in 3 global IT decision makers say securing their organisation's data is the most challenge task of their career.

The checklist above can help organisations better protect data and mitigate risks. By knowing exactly where each data set is at any given point in time, organisations are better able to gain transparency and accountability for the data. It is therefore important for organisations to assess their cyber supply chain risk concerning third- and fourth-party suppliers, in order to improve cyber resilience and risk management.

A way to keep close track of data as it moves from on premises data centres to public and private clouds is to use a standard portal management interface across all platforms which will ensure compatibility and visibility. Today, a good service provider will be able to provide this, along with managed security services and consulting to help organisations protect their data.

READ CASE STUDY: YMCA SINGAPORE

LUMEN



Making security the lynchpin of transformation

With the increasing complexity of networks and the growing amount of data, organisations have had to rethink cybersecurity over the past few years. No longer can they rely on traditional firewalls alone to protect their business assets and data, and even fairly recent developments, such as two-factor authentication (2FA) and multi-factor authentication (MFA), can be breached through sophisticated social engineering.

Today, cybersecurity cannot rely on standalone systems and needs to be baked into every layer of the IT stack. One of the reasons for this is that data no longer resides in a fixed location but flows to and from the various parts of the IT environment. As such, cybersecurity needs to be looked at from different angles, and needs to be handled using a range of different skill sets.

According to research commissioned by Lumen, 9 out of 10 global IT decision makers say application and data security is their #1 IT concern.

90% of global IT decision makers: Application and data security is their #1 concern

The three basic steps to cybersecurity

Securing an organisation's data can involve an array of different tools, technologies, and strategies. However, in its essence, cybersecurity relies on three key steps:

Monitoring & threat detection

To be able to identify threats, organisations must be able to monitor network activities, including cloud environment and applications, and user behaviour. This means using automation to proactively response to potential security threats with managed security services.

For effective monitoring, organisations should also move away from hardware-oriented solutions and adopt software-defined technologies that can protect today's distributed networks, Secure Access Services Edge (SASE) for example.

As the threat landscape becomes increasingly complex, managed security services, network security and cloud security have become priority for businesses to ensure their crown jewels are protected from insider and external threats.

Threat hunting

Besides monitoring and reacting to threats, organisations today must take a proactive approach and actively hunt for threats before they can be passively detected. This can be automated, using platforms such as Security Information and Event Management (SIEM) and other such platforms, which use AI to analyse data from previous threats to search for current threats.

Organisations with successful Security Operations Centre (SOC) can also respond quickly to threats and minimise the impact of cyberattacks. SOC can help to mitigate many cyber risks and greatly improve an organisation's security posture.

LUMEN

Majority of cyberattacks happen due to one of the 3Ms:

- Mistakes
- Misconfigurations
- Mismanagement

Training to reduce human errors

While IT assets can be protected with various technologies, human error can be both much more damaging and difficult to control. Unsuspecting employees might be subjected to phishing, resulting in data leaks. According to KnowBe4, approximately 88% of all data breaches are caused by an employee mistake.

Another aspect of human error occurs within the development environment itself, in what is known as the 3Ms: mistakes, misconfiguration, and mismanagement. For example, production data might not be purged from the development environment. Compromised APIs could also be a major security risk.

Today, with BYOD culture, it is critical for organisations to beef up their security awareness training to build a “human firewall”. Employees are the last line of defence and need to become an additional security layer when attacks make it through all the technical filters.

READ CASE STUDY: AUTO & GENERAL SOUTHEAST ASIA

Overcoming the APAC talent shortage

With the pace of digitalisation in APAC, many organisations are looking to rapidly grow their digital capabilities in the coming years, and will continue to face a struggle to fill crucial cloud and security roles. The education system is unable to meet the demand for trained resources, while skilled mature workers are hard-pressed to keep up with the skill sets required with each new development in technology.

Organisations have tried various ways to address the problem, including reskilling workers, offering apprenticeship programmes, and partnering institutes of higher education. However, doing so is often a futile endeavour, with freshly-trained talents being poached by competitors who are able to offer better salaries and employee benefits.

Fortunately, much of this work can now be executed by reliable partners, each of whom specialises in a specific domain. According to Frost & Sullivan, the shortage of security professionals in the market has led companies to outsource their security operations to managed security service providers. These providers offer managed services in deep domain-specific or software-specific expertise, and can alleviate the burden of hiring as well as the need to rapidly scale and innovate in the face of new technologies.

Ultimately, digital transformation is a journey

How do you start your DX journey and where does it end? The foundation of seamless digital transformation is adaptability. To gain adaptability, organisations need to transform their processes. This means adopting new framework to streamline workflows, improve efficiency and create unique user experiences that can attract modern consumers.

It is important to identify where the complexity exists in their operations and simplify them by using technology. Cost reduction, improved agility and flexibility all come with simplified and optimised IT infrastructure and processes. Seamlessly integrating current IT environments with the cloud to modernise IT and reduce complexity can drive more value from digital transformation.

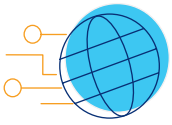
Finally, all these need to be built upon a holistic cybersecurity foundation that ensures end-to-end security. Simply said, to become digital-first is to leverage technology to transform, simplify and secure the business.

The way forward: Transform, Simplify, and Secure

At Lumen, we are focused on solving challenges faced by enterprise organisations. We support our customers who are ready to embark on their digital transformation journey by helping them to transform, simplify, and secure their business.

LUMEN

Our approach is built around four core foundations that will help you overcome the challenges outlined and to drive the most value in your digital transformation journey:



Network transformation

- Transform your network with improved flexible agility
- Simplify control of your enterprise network
- Secure your network endpoints with greater visibility

Cloud transformation

- Transform your business with scalable cloud capabilities
- Simplify management of your hybrid cloud environment
- Secure across cloud environments

IT modernisation

- Transform your business with modernised apps and infrastructure
- Simplify by reducing complexities in your tech stack
- Secure your IT environment with 24/7 protection against cyber threats

Security enhancement and cyber resilience

- Transform your approach to cyber risk management
- Simplify your cybersecurity strategy and operations
- Secure your critical assets proactively

Transform, Simplify and Secure your business with a trusted partner today.

Our mission is to digitally connect people, data and applications – quickly, securely and effortlessly. We enable you to make technology an integral part of your business strategy and help you succeed in an increasingly complex digital landscape.

Learn more about what we can do for you and support your digital innovation at **apac.lumen.com**.

apac.lumen.com | apac.mail@lumen.com