OPEN ALLIANCE for CLOUD ADOPTION

Topic: Post-Pandemic IT

Contributors:

Andre Schwan – T-Systems
Krishna Jadhav – Tech Mahindra
Mark Williams – TachTech
Matt Estes—The Walt Disney Company
Rommel Silva – PSU
Ryan Skipp—T-Systems
Shamir Charania – Keep Secure
Tom Scott—The Walt Disney Company

Contents

LEGAL NOTICE

This "**OACA Post-Pandemic IT - White Paper"** is proprietary to the Open Alliance for Cloud Adoption - A Linux Foundation Project (the "**Alliance**") and/or its successors and assigns.

EXECUTIVE SUMMARY

The world has changed in profound and unique ways. There is a new way of working with new rules and a new way of thinking when it comes to how value is measured. The recent virus pandemic has caused many businesses to change the way their people work, and businesses must rethink how to succeed in the post-pandemic world. Against this backdrop, abilities to deal with other future business interruptions going forwards must be built into the way we set up systems, processes, and services. One also must be sensitive to swapping long-term strategy for short-term survival tactics, thereby opening the risk of making detrimental or limiting short-term decisions. This paper considers a number of these approaches and business opportunities, and how modern IT can be harnessed to enable a new era of Business operation, competitiveness, efficiency, and innovation.

EFFECTS OF THE PANDEMIC ON BUSINESS

In most parts of the world, business activity suddenly became extremely limited with respect to office and production plant-based activity. One might even consider the complete enterprise as having become a "cloud business" – it is no longer just the data center that exists in some virtual environment – the whole business and all its units suddenly became distributed and "virtual", loosely connected and spread all over suburbs and homes and cities. This also affected income and suppliers. Providentially, all businesses were similarly and simultaneously affected, and so the option for consumers to simply transition to alternate suppliers posed less of an impact. Income from traditional clients and services has come under unexpected threats – loyal clients in many cases simply cannot pay (the full amount) for the services they require. As a result, they are being forced to downscale, forcing companies to rethink their product portfolio, service, and operating models.

Several "new paradigms" regarding "corporate working" have crystalized:

1. Wherever possible, staff are "Working from Home" (WFH), and many can't see why it can't remain that way in the future.
2. Staff have moved from desktops to mobile/remote devices, such as laptops and tablets.
3. Users are accessing the business applications and services via their private home networks in many cases through remote Access Point (AP) devices that replicate the "in-office" experience.
4. Software distribution and patching occurs via public communication routes, adding more momentum to consuming cloud SaaS-based services to circumvent corporate infrastructure and operations pressures.

5. Business data is accessed by staff over the Internet with unvetted devices where authentication and protection may be weaker.
6. Service desks must support remote staff and clients and offer support services in different quantiles measured more by time than results, engaging people who can drive their own delivery.
7. Technical support is not easily able to get to an endpoint device to provide help when needed and is under increased pressure due to the dispersion of endpoints.
8. Branch offices and Wide Area Network (WAN) connections are underutilized, with data movement patterns shifting to internet-based channels like direct internet access or SDWAN, reducing need for and capacity of traditional WAN services, (questioning how many buildings and WAN links are actually needed and how many can be permanently shut down).
9. Operations orientate towards staff coming into offices weekly for updates, training, and corporate updates in shifts and then working remotely, and thus not nearly as much office space required going forwards. Staff may also need to pre-book desk space through apps to enforce social distancing and safety expectations. (New applications for this are already appearing in the corporate landscape).
10. Measurement of user productivity has become management's next big challenge, especially where flexible working hours are concerned which force managers to adapt their management style towards outcomes-based management. New behavioral and AI-enabled applications are being implemented to influence staff productivity and maintain staff morale in remote working scenarios.
11. Budget expenditure decision making is focusing on efficient or critical business enablement, planning, and survival rather than long term strategy.
12. Staff is being retrained and repurposed to customer facing and critical business processes.

So, considering these paradigm changes in the workplace, how is IT continuing to enable the business?

1. Connectivity is via external gateways and VPNs that have been put under tremendous pressure.
2. Data Loss Prevention has had to evolve to deal with alternate data access and use patterns from users connected via the Internet. Staff training has had to evolve as well, highlighting security practices relevant in remote working scenarios.
3. Internal Business Applications have had to be adapted to become internet facing.
4. Due to reduced and reviewed IT budgets, expenditure is focused on minimum business enablement, targeted towards survival.

5. In some cases, there have been large migrations toward web-based directory services like Microsoft 365 and Google's G Suite. The usage of video conferencing and collaboration tools has accelerated tremendously.
6. With the erosion of the network boundary as an authentication factor, there is now more need for strong, centralized Identity and Access Management (IAM), together with Endpoint Protection Services (EPS), and Endpoint Detection and Response (EDR) services to help increase the "trustworthy-ness" of authentication decisions.
7. Security is being challenged to support an agile workforce, changing faster than it can keep up.
8. User password change policies and processes have been adapted.
9. Migration of email from on-prem to off-prem has accelerated.
10. Adoption of some of the cloud service providers' directory services has accelerated, with untested or uncertified trust relationships being established to the corporate environment.

All these mean that IT must quickly consider what minimum, yet critical permanent changes are needed to enable business, ensuring the business remains operational and competitive going forwards.

INTRODUCTION

Almost every business has changed their operational model. This document discusses many of these changes (the applicability of each change will differ between businesses – depending on if they leverage office workers who can work remotely, or if they run production facilities that require a varying degrees of onsite staff attendance to produce their products and services), and the reader will have to consider selectively which of the changes and opportunities below may be applicable in their specific scenario.

There are two major dimensions to these changes:

1. **Technology-related** migration towards a state that IT has generally defined quite well already, but possibly not yet achieved. Examples include:
    a. Increased use of Internet and Wi-Fi access (updated network policies).
    b. Web-enabled/facing applications.
    c. Desktop Virtualization for remote access and application use (and increased use of mobile devices).
    d. SaaS (and cloud) adoption.
    e. Data classification, governance, and access model enforcement.
    f. Trade-offs between using a "standard app experience" (e.g. SaaS services) vs high levels of customisation of on-prem applications (together with their maintenance implications).
    g. Application management and maintenance burden review (critical vs nice to have feature development trade-offs).
    h. Increased Security including:
        i. AI & Security Orchestration, Automation, and Response (SOAR IAM/RBAC)
        ii. Security Information and Event Management (SIEM) & SOC
        iii. User and entity behavior analytics (UEBA)
        iv. Application access including Multifactor (MFA) authentication
        v. Network rule changes
    i. Added user productivity or activity reporting.
2. **Businesses-related** changes in the way they work in general. Some examples include:
    a. B2B dependency and partnership mapping and relationships under new structures and governance.

b. Business transaction model changes which increasingly include more trust and use of digital recordings.
c. Elimination or optimization of branch offices/buildings to reduce operating costs – an all Internet world – reduction/repurpose of commercial real estate.
d. Verification of the enterprise application landscape and the minimum viable landscape to support (critical) business functions.
e. Restructured operating and process models.
f. Brand re-creation around core services and differentiators.
g. Identity-based controls and validation at the business level (no more physical signatures and handshaking) – video and app-based verification.
h. Addition of health and tracking apps into core landscape.

This paper focuses on items that have changed the way businesses work, with special consideration for changes in cost-effective operation and survival, increased flexibility, and competitiveness.

In each area we will consider appropriate dimensions from the following list:

Dimension	**Achieved Through**
Cost Changes	Changes that result in cost savings at either operational, production, or expenditure levels.
Efficiency Gain	Changes that have enabled business to reach their objectives more easily, often by avoiding barriers or shortening processes.
Flexibility Gain	Changes in the “usual” processes that have made working and decision making faster and easier for users, customers, and partners.
Optimizing	Elimination of unused functions and features, and/or alternatives, down to one simple minimum viable (often internally shared) solution.
Managing Barriers	Instead of fighting or eliminating barriers, using them as decision points or forks in a process.

PROBLEM STATEMENT: CHANGED BUSINESS OPERATION AND IT CHALLENGES

As users have (suddenly) migrated to working remotely (from home), many businesses have realized that they are still able to maintain an acceptable level of productivity, and that having a percentage of the staff rotate into the office in a highly shared environment can offer them significant infrastructure savings. This model places significantly increased pressure on parts of the IT infrastructure and services though, and thus requires additional catering to the network, internet capacity, and firewalls, as well as access to applications via web and fat clients. Users must access business applications and data remotely leveraging (insecure) public networks and services, while partners interact via similar channels. Business security policies, infrastructure, and applications have not been completely ready for this sudden change, and several approaches and methods must be identified to help managers deal with both the financial and technology problems, and opportunities that result.

MOBILE/REMOTE USERS:

Users have (in many cases) had to migrate from desktop workstations to laptops and from the office to home. This brings several considerations and opportunities:

Dimension	**Achieved Through**
Cost Changes	• Conversion to use of externally provided/contracted "walk-in support services" or "post in unit exchange services" for users' devices vs use of "internal workshops", with associated cost model changes (or additional stock holding), for maintenance. • Increase in use of remote productivity tools to maximise collaboration (requiring many organizations to invest in these tools for the first time) – e.g. MS Teams, Zoom, Webex. • Reduction in infrastructure costs through reduced onsite staff, such as parking space, electricity and air-conditioning, LAN, cafeteria, and printing where users are learning to work with online documents. Desktops are also not left running overnight, reducing smooth and UPS power requirements. • As services are "pushed" to the edge, there can be more "per-active user" licensing type arrangements than a big/single purchase, since access methods and tools are changing.

	• As businesses switch from CapEx to OpEx, both security and networking services need to be realigned to accommodate the new cost and operating models. • Increases in costs as laptops and tablets are typically more expensive than desktops. • Laptop screens (particularly in models with reduced size) can be quite small, and this has an intangible effect on productivity. • Increase in connectivity costs from personnel's homes which is offset by the mentioned reduction in branch or office costs.
Efficiency Gain	• Remote self-help facilities enabled at the helpdesk for users – e.g. password resets, software re-imaging or scheduling, and downloading updates into slots appropriate to users, when they are connected via cheaper network connections (but within acceptable timeframes to the company). • Office desks becoming shared, with staff rotating in for a day a week, typically for team meetings resulting in organizations reducing the overall office space that they rent/use. • With the lines between home life and work life being blurred, many organizations are experiencing an increase in discretionary hours worked by their staff. Discretionary time is typically not remunerated, increasing output at little or no additional cost.
Flexibility Gain	• There is much less "LAN" support at the enterprises' offices and a reduced need for local switch equipment. When users do come to the office, they now usually connect via Wi-Fi. • Enterprises often move to equip key remote users with mobile LTE-enabled routers, which allow QoS management, closer firewall and policy management, and intelligent separation of traffic between internet and local data center-based applications. • By breaking the dependence on physical location-based delivery, organizations gain operational flexibility by having more options and combinations to draw on as they adapt their products and delivery methods.
Optimizing	• Need for branch offices is reduced to only the client-facing portions in many cases.

	• Getting a corporate "image" onto a laptop with appropriate security software and configurations - IT has to shift from "imaging" a hard drive to deploying a set of software and running configuration scripts. • Configurations for standardized devices must be well tested and defined by the IT team so that devices can be monitored for compliance with policies (if each laptop requires different drivers, this can be a challenge, so standards are essential). • Migration to the use of cheaper online helpdesks (possibly with less rich functionality but at a minimum viable level for user online support and self-help) integrated with some of the desktop tooling. • Safely accommodate a "Bring Your Own Device" approach through use of a virtual desktop service. • Evaluate DaaS (Desktop as a Service) options which may be required for certain workload types (heavy GPU, etc.).
Managing Barriers	• Initially, large-scale procurement of laptops is challenging, but it does prepare companies for being ready for disasters and other location-specific issues and distributes some risk. • End-user support means that IT must travel to the user if they can't solve a problem via remote control – which means more time required for fewer support tasks. Timely shipment of freshly imaged devices to remote users may ramp up to minimize end-user disruption. • Although new office requirements include social distancing features and increased partitioning/screening, only having to cater for a small percentage of staff being onsite at any time can allow significant savings in infrastructure. • Increasingly, businesses need to rely on commodity hardware/software to support initiatives. IT is no longer in the business of issuing bespoke configurations.

NETWORK CHANGES:

Companies have been migrating from on-prem data centers and traditional WANs to cloud service providers over the past several years under the "Cloud First" principle. Today that is no longer optional for many companies. Due to reduced revenue streams and operational staff reductions, companies are seeking ways to reduce cost and overhead, and the "corporate network" is on the chopping block. The cost and overhead of supporting owned networks, i.e. data centers and network infrastructure (WAN's, LAN's, physical cabling, internet connections, Wi-Fi, security services for "in-house" virtual networks) are becoming cost prohibitive, and many companies are seeking alternatives to traditional networking architectures.

Dimension	**Achieved Through**
Cost Changes	• As businesses adjust their product sets, they can select supporting technologies that, by design, reduce network spend and open the door to new channels to market. E.g. adopting cloud-based SaaS solutions, opens how different classes of users can interact with the organization's data and systems, moving traffic from traditional high cost WAN infrastructures to lower cost internet-based software defined network (SDN) and network function virtualization (NFV) services and a PAYU basis. • Moving to Cloud Service Providers (CSP) for infrastructure services can eliminate hardware cost and overhead. Capital expenses in which hardware is depreciated over several years is converted to an operating expense which can provide an immediate tax benefit. • Leverage CSP's offering to take on "non-differentiating services" such as networking architecture and support.

Efficiency Gain	• One of the biggest benefits of cloud services offerings is "elasticity" in which operational network overhead can be greatly reduced while delivering (in near real time) network services to meet demand. These include:
	  ○ Software Defined Networks
	  ○ Network Function Virtualization
	  ○ Increased automation to provision/deprovision as needed

Flexibility Gain	• Network services that respond to demand provide an opportunity to companies faced with a lack of resources, enabling real-time response to market changes. • Implementing networking services from cloud service providers offers many companies increased flexibility in how network resources are provided and consumed. E.g. users end up working on private and public Wi-Fi. • Typically, QoS is location dependent, depending on the network provider. Some remote Wi-Fi services and devices enable local "self-help" function hosting from the help desk and QoS capability, which are useful for leaders, team management, executives, and for distributed help desk services.
Optimizing	• Network optimization traditionally required a company to rearchitect their existing infrastructure. Today, network optimization can be provided as a service from cloud providers who can offer various tiers of service which can be tailored and applied to the needs of individual business areas, rather than a "one size fits all" maximum feature solution.
Managing Barriers	• Many businesses are increasingly encumbered by unused local network infrastructure that needs to be operated, maintained, and administered. With a reduced workforce many companies are prioritizing only the administration of core areas, and onsite users are moved to these areas, with other areas disabled. With the promise of Infrastructure as Code (IaC) and Serverless Architecture (SA) offerings, many companies are scaling services directly in line with active business. • Request for Proposals (RFP) and brand selection choices are limited to contracted cloud service suppliers' offerings, which are supported by corporate procurement and compliance policy changes. This reduces time-to-service and people evaluation efforts. • Users use home Wi-Fi at their own cost, rather than the company sponsoring it, but consequently, use of cheaper or insecure

	public Wi-Fi hotspots happens – define policies that are automatically applied based on the access channel.

SECURITY CHANGES:

Security must adapt or risk becoming isolated and disassociated from current operations. Some of the changes are subtle while others are more dramatic. While companies may be recovering from the aftermath of Covid-19 they need to take stock and reassess the risk landscape for high-value data, applications and services, as these (tolerance/disposition for risk, access models, questioning about the security of the code when accessed externally or via public routes, devices used for access) have changed.

Dimension	**Achieved Through**
Cost Changes	• Identify core and "nice to have" functions in Security, and then consider reducing to only core functions, and contracting the rest externally, as needed, from specialists. • Know exactly what must be measured and managed. Services require the same amount of operational support as "pre-pandemic". Typically, if you put one aircraft in the air or bus on the road, or the usual fleet, you still require all (100%) of the enabling services and support to be in place. Re-examine exactly what tools and functions are needed to keep services running, at minimum viable levels, i.e. eliminate the spare capacity and unneeded activity by means of contracting capacity and services (often virtual/cloud) to deal with variability. • Leverage and consolidate well-integrated tool suites and automation (that might previously have been underutilized) to reduce costs of multiple partially utilized tools - and of course this may then drive a reduction in resources as well. It is amazing how much "shelfware" is paid for but un-utilized in big companies or only partially utilized in pockets. • In utility-based cloud models, reduction in use equates to reduction in cost. This however does not translate to all technology stacks, especially security. Security costs increase

	with the management of additional risk to secure remote locations and new channels due to tool and policy updates.
Efficiency Gain	• Remote access to resources can be more efficient if access is leveraged from internet endpoints that have appropriate bandwidth to support the required performance to meet workload requirements. Moving to cloud solutions that are especially designed around this type of connectivity can increase efficiency, also leveraging integrated access and authentication services designed for internet access, e.g. Microsoft 365 using federated ID services.
Flexibility Gain	• Remote users now access corporate applications remotely (with additional security needed for VPN and federated authentication). Enhanced security is needed to access applications from any internet-connected device securely and provides users with greater flexibility to access corporate resources remotely. This can yield improved responsiveness to customers.
Optimizing	• Update corporate compliance policies to work with all selected Cloud Service Providers (CSPs), to enable consistency (reduce number of policies to maintain) and manage compliance across multiple providers.
Managing Barriers	• The largest contributor to increased security risk is lack of knowledge. Many organizations are moving into cloud-based systems without having deep understanding of how to do so securely. Training takes time, and companies should train resources tactically and strategically, enabling them to learn the required new skills in stages or source skills from a specialist supplier for the interim. • With increased access paths and more sophisticated risk, Security battles to control balance between attacks and defense. Analyze and map this risk and the threat profiles to help organizations realize where to apply limited resources to manage risk.

	• Moving to distributed cloud environments requires enhanced endpoint security. Endpoints that lack enhanced security become barriers to accessing/locating company resources in the cloud. • Use of spare corporate service and infrastructure capacity can be applied to enable third parties, partners, clients, educational services, training, social development, and similar formal non-profit (organizational) services (leveraging governance for approval), which brings goodwill and positive publicity. • Blocklist and safelist access to business data and systems must allow for traffic from the opposite directions than before over different paths and consider individual device compliance. • Threat Hunting activity needs to extend to new environments since users now work from (shared) home networks where potentially insecure devices may be co-located, and this must happen with the users' permission or via an alternative technology or approach which also benefits the remote user.

GOVERNANCE & COMPLIANCE

Governance and Compliance work together to measure risk, adherence to policies, and manage uncertainty. In today's uncertain times, "uncertainty" is the norm. Policies and regulations all must be adjusted to the "new" norm, which has yet to be defined. Business will need a coordinated strategy for managing Governance, Risk, and Compliance (GRC) in this new paradigm.

Dimension	**Achieved Through**
Cost Changes	• Added process and tools mean the cost of measuring and controlling governance and risk will increase as complexity (dispersion) of the operational environment (applications and network) increases. • Businesses are looking for ways to incentivize "delivery" from employees. Traditionally people are paid for "activity", i.e. number of hours working to produce an outcome. However, today this is not as easily captured, and paying employees for

	deliverables and outcomes, rather than activity, is one way which companies incentivize increased efficiency.
Efficiency Gain	• Conversion to a measurement-based payment model drives staff to focus on achieving outcomes and deliverables (rather than hours at a desk) which increases business efficiency, but this requires contract amendments and policy changes.
Flexibility Gain	• Policy updates to allow access from alternative locations, with pre-determined conditions (e.g. only via VPN, or at certain hours, or limiting access to data and services depending on the endpoint state and access path). • Policies need to be updated to both enable users and accommodate service delivery to customers, via different access points and routes.
Optimizing	• Define which decisions and policies really need to be signed off by central or executive teams and distribute the rest to the appropriate decision makers - e.g. application owners own the data and are responsible for compliance and locating/hosting it according to predefined corporate guidelines and rules. • Create a set of guidelines to help distributed managers make decisions rather than controlling everything centrally. • Reduce the size and length of decision meetings – invite the relevant people to make decisions and inform the rest of the team by means of collaboration tools. • Rapid working team members deliver large volumes quite quickly, but they often need the slow, solid, steady, and methodical team members to pick up errors and perfect their output – structure remote worker task allocation to take advantage of the specialization and aptitude of each individual in a team so as to achieve an overall quality output with minimized rework.
Managing Barriers	• Users work in uncontrolled spaces (whether exposed to family or public) on sensitive company systems and data and discussions – confidentiality is more challenging. Define privacy needs in

	advance of a meeting so that users can address their privacy requirements (e.g. isolated location or display positioning) based on the sensitivity of the topics to be addressed. • Distribute relevant decision making to line management regarding policies to be applied to their staff. Many generic policies may not really apply to all teams. • Define policies per business function that are automatically applied when a user accesses that system, detecting their access routes and which policy to then apply rather than blanket policies applied to all applications and functions and access.

BUSINESS FUNCTION & APPLICATIONS

Many business functions and associated data that were previously strictly confined to the "inner sanctum" of the secure enterprise network must now be accessible to users accessing them from remote, home, or public networks. In many cases this presents a real challenge, both in terms of protecting corporate IP and exposing corporate data. Some applications are not internet facing and can be moved over to more accessible SaaS options. In order to manage this, we consider application and business function services below

Dimension	**Achieved Through**
Cost Changes	• Use the opportunity to rationalize the application stack and choose a closely matching COTS or SaaS solution at a discount rather than maintain heavily tailored solutions. Review logs to determine the real usage of each application or function in the business landscape. • Identify duplicate applications and consolidate down to one that provides the most relevant functionality. This reduces operational burdens which arise from limited direct access to service consuming endpoints, support of duplicate automation, and scripting to support multiple versions and distribution packages. • Address and remove the "holy cows/golden cows" which may no longer hold the value that they are purported to hold –

	duplication results in higher licensing, staff, and data center / cloud costs.
Efficiency Gain	• Leverage more SaaS and less own internal development • Use opportunity to align to new or centralized common simple processes, while people are receptive to a "change mode". • While staff are receptive to this "change mode", use the opportunity to align to new or centralized common simple processes. • Distribute decision making authority to the relevant roles but with the associated responsibility allocation and governance controls. • Reduce the maximum size of meetings to only what is required and inform the rest of the staff by means of proper records (memorandums / minutes) or collaboration systems (e.g. Confluence, SharePoint, Slack, etc.).
Flexibility Gain	• With application rationalization, complexity in the landscape is reduced, making it easier to make major changes which might be needed as the business readjusts its product portfolio to survive. • Application and landscape rationalization reduce complexity of DR, and the capacity required for DR is reduced. • By expanding the manner and origin personnel are permitted to access organizational resources, many organizations can significantly increase their operational flexibility, and in time even how they execute their core product and the supporting processes. • Drive towards loosely coupled applications to enable function replacement and reduce dependency on integration specialists.
Optimizing	• Reduction of the number of versions of applications to support and license reduces the burden on support staff, possibly leading to savings – especially if some support, which may be contracted externally, can be optimized. Examples extend to multiple versions of office automation tools, duplicate accounting and budgeting tooling, and many diverse database types (e.g. MS SQL, Cassandra, MongoDB, etc.).

Managing Barriers	• Data Classification – apply the business definitions according to governance requirements and distribute responsibility to roles accordingly. • Access from "the outside" vs "the inside" - leverage and trust the governance, definitions, and controls, based on clear responsibility being assigned to managers who own business functions. • Use of collaboration and sharing tools must be formalized via governance and policy that prevents unnecessary exposure of business processes and applications via new interfaces. • Fat clients can enable better security control (especially regarding company data access and protection) than web applications where the data may be cached or stored in clear text format. • Health and tracking apps now become a part of the landscape to enable users to work safely and be appropriately informed of potential health risks.

CONCLUSION

The transformation required to deal with this post-pandemic world in which we must live for the next number of months, and possibly years, is forcing accelerated rethinking of how businesses operate and what they focus on. Against this backdrop, similar ability to deal with other future business interruptions going forwards must be built into the way we set up systems, processes, and services. The factors discussed in this paper identify some of the early learning, which some of our organizations have applied. This has helped create capabilities and operational improvements in dealing with the new ways of working and delivering products and services.

One must be sensitive to swapping long-term strategy for short-term survival tactics, thereby opening the risk of making detrimental or limiting short-term decisions. It remains to be seen how well companies navigate these choices to realize an overall positive business outcome.

These uncertain times have also seen the rapid reconfiguration of business strategy, operations, and decision making to deal with the pandemic-induced crisis, create approaches that will support/restore business momentum, and prepare to navigate similar interruptions in the future. This thinking is core to decision making going forwards.