

Digital Transformation During Lockdown

Ioan DRAGAN

The Bucharest University of Economic Studies

Dragan_ioan1989@yahoo.com

This paper presents some preliminary findings of the digital transformation methodology innovation research done as part of the PhD studies. The COVID-19 pandemic changed the way we work and a large majority of the companies found themselves not prepared to move to a full remote or hybrid workforce model. Traditional software platforms and components are not designed for remote use, nor offer the right information protection and governance features. This paper presents a study of how business executives see the future workplace and a methodology for short term mitigation and long-term planning in the context of hybrid workplace.

Keywords: Digital Transformation, Collaboration, Cloud, End User, Education, COVID-19, Workplace

DOI: 10.24818/issn14531305/25.1.2021.07

1 Introduction

Digital transformation, also called, digitalization, is the integration of digital technology into all areas of a business, fundamentally changing how it operates and delivers value. Digital technologies are changing the way businesses operate, and this change is faster than the pace of transformation. Such radical changes are typically undertaken in pursuit of new business models and revenue streams, driven by changes in customer expectations around products and services as well as digital upstarts that are upsetting traditional industries, leveraging scalable technology and participative networks.

Digital transformation is not new, but the conversation has shifted to how rather than why. Digital business reached a tipping point in 2018 as organizations scaled their digital capabilities. Despite the challenges of the COVID-19 pandemic, enterprises around the world are making significant investments in the technologies and services that enable the digital transformation of their business models, products, and services. According to surveys done by Mulesoft [1], more than three quarters of managers and more than half of employees say their organizations are engaged in digital transformation. To help move digital transformation forward, having the right digital-savvy leaders in place is considered key. Even as IT budgets shrink due to the COVID-19 pandemic, the crisis has

underlined the importance of digital transformation and accelerated its pace for many organizations.

However, organizations struggle to turn their digital ambitions into reality. There is a gap between expectation and results. Inconsistent sponsorship from leadership is a top challenge for those leading digital transformation and cultural issues also pose notable difficulties with companies that span multiple countries or even continents. Despite the concerns, many companies embrace the change digital technologies offers. IDC [2] forecasts global digital transformation spending will reach \$1.3 trillion in 2020, and Markets and Markets expects the digital transformation market size to grow to just over \$1 trillion by 2025. Connecting consumer experiences and data-driven decision making are key drivers of transformation efforts.

In a digital business transformation context, business functions, processes, assets, models, and activities are interconnected. This is an essential aspect of digital transformation. Ultimately, success in the digital age lies not in the efficiency of technology but in the dexterity and adaptability of the people who use it. Digital is an enterprise-wide strategic priority, but there's a lot of work to be done to get it right. The global COVID-19 pandemic has simultaneously slashed IT budgets and revealed the urgency of reaching consumers digitally as quarantines have upended traditional ways of

doing business across most sectors. A survey by McKinsey found that the most commonly mentioned objective for digital transformations is digitizing the organization's operating model, cited by 68% of respondents.

Historically, every disruption brought significant change and improvement to the ways of working and to the quality of life:

- The first industrial revolution started at the end of the 18th century and was led by the invention of the steam engine. While the mechanization of the agriculture was not seen at first as an improvement for the agriculture workers, it later allowed them to explore other industries with higher wages. Also, this improved the mobility between countries by developing railroads and trains. The disruptor was the technology itself: new ways of producing and utilizing energy. This process of transformation took about 100 years.
- The second industrial revolution started at the end of the 19th century with the help of new energy sources: electricity, gas and oil. The massive technological advancements allowed the energy sources to be lighter, cheaper and easier to store and transport. The democratization of energy and communication allowed companies to expand to other countries and even continents much faster than ever before.
- The third industrial revolution happened in the middle of the 20th century with the emergence of the nuclear energy and the programmable logic controllers. As with the other industrial revolution, the adoption of these new innovations was driven by value to the community and took years. What we're observing is that the adoption cycles have substantially decreased from 100 years, to 50 and then 20 and the impacted percentage of the population has steadily increased.
- The last industrial revolution, called Industry 4.0. This was driven by something we all use every day: The Internet. As with all others, the initial adoption was value driven, the time to adopt has significantly decrease, but only a part of the large population received full benefits from

adopting it. The complexity of the technology is much higher and some traditional industries are not able to take full benefit of it. Industry 4.0 has an additional catalyst that others did not: a pandemic that required lockdown and accelerated use of technology to ensure business continuity.

The paper aims to identify the factors that are critical for enabling remote work in traditional technologies and help companies protect their employees in a pandemic. These times are unprecedented and pose significant challenges but also opportunities to improve the quality of life for information workers, expand the recruitment area outside of large cities and help fill in the income gap between high cost labor markets and low-cost labor markets.

2 Current Context of Remote Working

The global COVID-19 pandemic has simultaneously slashed IT budgets and revealed the urgency of reaching consumers digitally as quarantines have upended traditional ways of doing business across most sectors.

Whether for business, educational, or personal purposes, it is clear that people have turned to digital channels to fulfill many aspects of their lives. As a result, customers are no longer expecting only the basic experiences they were offered before; instead they have developed much higher personalized and digital need. This is why all businesses, regardless of industry or size, have to accelerate their digital adoption, transform their operations to meet consumers where they are and give them the experience they expect. While this is an unprecedented threat to the human health, it poses a great momentum to transform multiple traditional businesses that were not adequate for the new Industry 4.0.

Many business are exploring different strategies for a phased return to the office when the medical safety allows it, 23% of the employees [4] say that they would like to work more from home. This means a high digitalization of operations that allows the company to run uninterrupted with a part or all workforces being remote.

PwC ran an extensive survey in January 2021, almost one year after the lockdowns have started to affect the workforce around the world [5]. The company evaluated a few factors: executive and employees' perception on work from home experiment results, returning to the office timelines, future of remote and office work and company culture impact. First and foremost, the evaluation of remote work shows different results between what employee and what employers think (Fig. 1) [5]. 83% of the employers consider that remote work has been successful, whereas only

71% of the employees consider the same. The disconnection between employers and employees has been attributed to lack of preparation and knowledge on how to manage "the new normal": building a schedule, mental health and separating work from personal life. Safety and Health Magazine [6] ran a survey with more than 4000 employees in the US and found that 84% of the workers consider mental health more important than a year ago and 32% consider that stress is top of their health concerns. 33% of the employees reported symptoms of anxiety or depression.

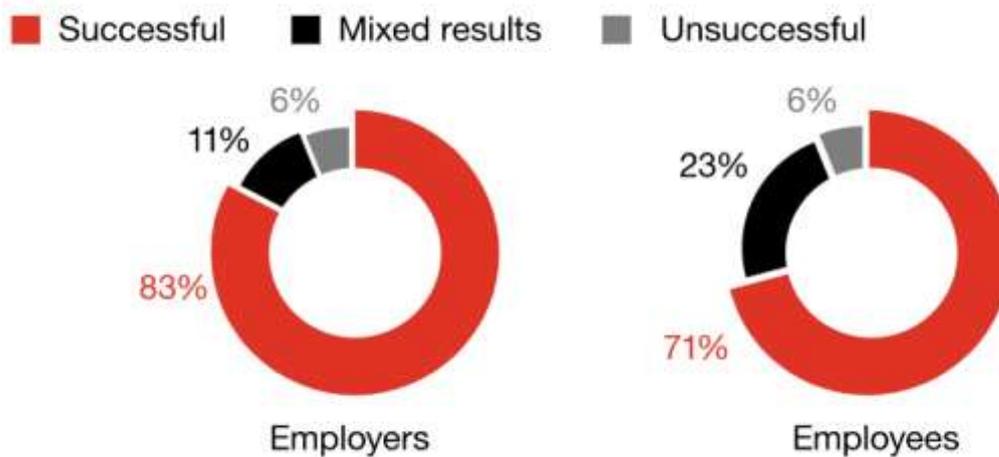


Fig. 1. Remote work has been a successful experiment

The next important factor evaluated by PwC is the workplace culture consistency. There are valid concerns that companies will not be able to build, maintain or change their culture in a remote working environment with current knowledge and abilities. The consensus is that offices are here to stay, but their main purpose will significantly change in the next years. There is a low appetite to return to the office

in the same pre-pandemic format. Only 13% of the executive active support this model. With regards to culture building, the majority of the executives still consider "weekly" presence to the office. A total of 84% of executives consider at least 1 day per week presence in the office as being critical to maintaining the culture. Fig. 2 presents a breakdown of the results.



Fig. 2. Keeping a strong culture - survey breakdown

Last, but equally important is the timeline to return to the office. The expectation to at least return partially to the office differs depending on the age group, but the numbers seem to be rather surprising: 55% of the employees mention they already spend at least half of their time in the office. The rollout of vaccines is raising confidence on medical safety, but there is a high level of uncertainty on how to successfully manage the return to office or at least a hybrid workplace model. Definitely, the workplace structure should change and have less populated spaces to ensure safety. Interestingly, the survey results show a discrepancy between the expectations and what is actually happening in the field. While employers and employees consider to a large extent that this has been a successful experiment and there is a strong appetite to continue investment in remote working technology, a large majority of employees wants to return to the office. This leads to the conclusion that the future workplace will be a hybrid one, with

flexibility to choose where employees will be working from. Thus, employers will have to transform their operation models to accommodate remote work and seamlessly collaborate without restrictions in a hybrid model.

3 Technology Associated with Remote Work

The IT departments face their own unique challenges, such as adapting to a world where IT no longer has a monopoly on technology expertise, budgets, deployment, and support, boosting business performance by exploiting the growing digital dexterity of employees, and aligning digital business investments with the rapid rise in the technical competence of all employees. IT is being asked to transform their businesses, but not getting the budget to do so, finding them in a situation where additional scrutiny is needed on purchasing, capital expenses and long term investments. Many of them accelerated the purchase of cloud services as those do not require significant

upfront investment. The pay-as-you-go model allowed companies to move online in a matter of weeks, boosting the demand for collaboration platforms.

To have a better understanding of the components needed, this paper summarizes the minimum requirements for a company to function in a hybrid model driven by cloud services:

a. **Secure identity platform** – 81% of all hacking related breaches are driven by compromised credentials [7]. Also, 15% of the phishing victims fall for the second time for the same attack. Compromising the identity platform can stop any activity happening in the business operation platforms. The main objectives of an identity platform are: user management, authentication management, authorization management, access management and auditing, all while keeping users safe from different types of attacks.

All leading cloud vendors provide their own identity platforms: Microsoft Azure Directory, Google Cloud Identity platform, Amazon Cognito and others. Also, there are some niche providers like Okta and Ping that provide identity platforms as a service.

b. **Endpoint management platform** – traditionally, user endpoints were managed onsite with tools like System Center or different proprietary ones. The main objective of such a platform is to easily distribute software, updates and settings and to help automate the endpoint setup. Modern cloud platform offers those services out of the box, offering a “zero touch” experience for the IT personnel (the device can be shipped directly to the end user and the setup will be done remotely in an automated fashion without them having to “touch” it).

Some of these leading companies have reported increased usage between December 2019 and March 2020, led by the migration from on site to online. Some examples of Endpoint Management platforms below [8]:

Microsoft offers Enterprise Mobility + Security, a mobility management and security suite that combines endpoint management with identity and access management, threat protection, information protection, and a cloud access security broker.

MobileIron offers organizations quick and easy access to onboard devices and provision them over the air with all of the apps, settings, and security configurations needed to protect any iOS, macOS, Android and Windows 10 endpoint across the digital workplace.

Sophos Mobile is a unified endpoint management solution that helps users manage and secure traditional and mobile endpoints. The tool integrates natively with endpoint security programs and supports management of Windows 10, macOS, iOS, and Android devices. Citrix Endpoint Management is a unified endpoint management tool that acts as a consolidated console to manage diverse end user deployment options, including BYOD, Office 365, and Windows 10.

As shown above, most of the platforms offer similar services, including some kind of endpoint security service.

c. **Collaboration** – this platform helps people get work done together. This is probably the most requested type of service during the initial lockdown. The leading companies reported increase in usage: ZOOM 2000% Dec-2019 to Mar-2020, Cisco WebEx 250%, and Microsoft Teams 600% from Dec-2019 to June-2020.

Collaboration is the new normal in the workplace. These platforms could offer everything from cloud document storage for managing daily tasks, to video conferencing for online meetings, and all work just as well on mobile devices as well as desktops and laptops. Below there are some that have been growing recently:

Microsoft Teams is a collaboration app that helps teams stay organized and has conversations - all in one place. It offers persistent chat, document-based collaboration, online conferencing and telephony services. It is the natural evolution of a number of products that Microsoft has been developing over the years: Skype for Business, SharePoint, Yammer and others.

Zoom is another platform that has been growing significantly in the past year. It's a cloud platform for video, voice, content sharing, and chat. It runs across mobile devices, desktops, telephones, and room systems.

Cisco WebEx is a video conferencing and collaboration product suite. As with all the others, it represents a cloud-based collaboration platform, a merger between the WebEx Meetings, WebEx Teams and Cisco Spark collaboration application.

Google Meet is a video-communication service developed by Google. It is one of two apps that constitute the replacement for Google Hangouts, the other being Google Chat. Together with the other G Suite services, it builds up Google's solution for team collaboration.

The three solution areas above have been identified by surveyed customers as being critical for enabling remote work. Obviously, depending on the complexity of the business, multiple line of business applications needs to be published, updated or even replaced to be suitable for remote work. Customers had to quickly adapt to the new environment and take quick decisions on what is critical and what is nice to have.

Next, the paper proposes a methodology to manage remote working transition and define a strategy for short term risk mitigation and long-term enhancements to the experience offered to employees.

4 A Unified Methodology to Manage Remote Working Transition

The objective during the lockdown is to continue the information workers activity with minimum impact and to ensure security and safety of the data they are working with. In the previous section the paper has enumerated a number of critical software components to ensure a smooth transition. Below are 6 critical steps to ensure your success:

1. **Run an inventory of the essential software and platforms in your business** – all companies have a mix of legacy platforms that are due for retirement and modern, cloud services that require little to no maintenance. Unless the company is a recent startup that was born in the cloud, there will be legacy, on-premises applications and platforms that are not remote access friendly. While the application inventory is a requirement for data protection

compliance, most companies do not assess them past their data flows. The assessment should contain the user groups that require the application, criticality and remote accessibility options.

It is recommended to start the assessment with the three critical platforms mentioned in the previous section and identify the answers to the following questions:

- Can users authenticate remotely to any applications published on the internet?
- Can the IT administrators manage remotely the user endpoint?
- How do users collaborate? Is the communication and document sharing efficient?

2. **Reevaluate your customer needs and remove any unnecessary software and platforms** – customer needs and behavior are rapidly changing in an unpredictable manner due to the pandemic lockdowns. Companies have to constantly reevaluate if their customer needs are met and quickly adapt to what they're searching for. Some software platforms will quickly become obsolete and have to be replaced to meet their customers where they are. Also, this is a great opportunity to remove any unprofitable business lines and open new opportunities.

3. **Assess the customer data your employees have access to and plan for the information protection policies** – traditionally, some companies enforced data privacy by strict policies with their on-site workforce, restricted internet access and in certain situations, no access with video cameras on site. With remote working, those policies are obviously obsolete and have to be changed into modern, software driven information protection. Modern information protection and governance relies on minimizing access to information for each individual and protecting against accidental loss. The collaboration platforms mentioned previously offer different options for data loss prevention and identification of private data that is being

stored or share inappropriately (e.g. Microsoft Information Protection and Governance). Data privacy officers play a key role in defining controls and policies to stay compliant in the hybrid workplace.

4. **Mitigate short term needs for remote working** – based on the assessment done at point 1, a short-term mitigation plan has to be executed to ensure business continuity. The mitigation activities can consist of implementing software or workplace shifts to protect employees during the lockdown times. Some examples of mitigation activities, but not limited to:
 - Invest in cloud services to cover the basic needs of the company
 - Securely publish over the internet line of business applications that are critical to run the business continuity
 - Use a mix of on-premises and cloud to publish applications while securing them with cloud services. E.g. Secure cloud application proxies that ensure DDOS and authentication protection
 - Change business processes that require the use of on-premises applications that can't be published to be used from regularly to rarely
5. **Plan for long term transformation** – while short term mitigation plans are good for ensuring business continuity, the end goal is to have an effective hybrid workplace setup that allow employees to seamlessly collaborate without the limitation of being on-site. This requires a rethink of business processes and supporting software platforms to achieve this goal. Generally, companies are moving off on-premises software as it requires on-site presence to manage infrastructure, it can be a single point of failure in case of incidents and requires high upfront investment.
6. **Ensure leadership readiness for remote management** - Organizations are starting to understand that while technology is important, alongside customers, their organizational culture is at the center of any transformation. If people lack the right mindset to change and the current

organizational practices are flawed, digital transformation will simply magnify those flaws. CIOs play a leading role in empowering the digital economy; however managers and employees will need to navigate the digital frontier together, which requires a new set of leadership skills. Management's challenge is to figure out how to capture the benefits of digitization while minimizing the costs –and making sure those costs are shared and not borne disproportionately by one group.

5 Conclusions and Future Research

Extensive research on digital transformations has shown that the success rate for these efforts is very low: less than 30 percent succeed. This year's signals suggest that digital transformations are even more difficult, even though companies have an extra motivator to do it. Only 16 percent of respondents say their organizations' digital transformations have successfully improved performance and are also equipped to sustain the changes in the long term. [3]

In a digital business transformation context, all aspects of business functions, processes, assets, models, and activities are interconnected. This is an essential aspect of digital transformation: the interdependency and inter-connectedness of software, people and culture. Ultimately, success in the digital age lies not in the efficiency of technology but in the dexterity and adaptability of the people who use it. Digital is an enterprise-wide strategic priority and should be definitely treated as such.

The research identified a list of patterns that apply to almost all traditional industries: digital transformation is viewed only as a replacement of technology. The desired approach is to use the opportunity of having new technologies to transform the way companies deliver value to their customers, remove unprofitable business lines and generate new streams of revenue. This paper offers a short-term mitigation option to manage the crisis generated by the COVID-19 pandemic and leaves the research space for a more exhaustive study to identify a complete digital transformation

guide for companies that want to make the leap into Industry 4.0.

As mentioned in the first section of the paper, the pace of transformation is accelerating. In the first industrial revolution, the transformation took about 100 years. We're looking at current technological advancements that need less than 10 years now to be adopted. Companies have to increase their agility to match this kind of change pace.

References

- [1] Mulesoft, "Top 7 digital transformation trends shaping 2020", 2021
- [2] International Data Corporation (IDC) Worldwide Digital Transformation Spending Guide, FRAMINGHAM, Mass., May 20, 2020
- [3] H. de la Boutetière, Alberto Montagner and Angelika Reich, "Unlocking success in digital transformations", McKinsey, October 2019.
- [4] Global Web Index, "Coronavirus research", April 2020
- [5] PwC's US Remote Work Survey "It's time to reimagine where and how work will get done", January, 2021
- [6] Aetna International, "Global Employee Health Study Data", November 2020
- [7] "Verizon 2017 Data Breach Investigations Report"
- [8] D. Hein, "The 12 Best Unified Endpoint Management Solutions for 2020", Solutions Review, February 2020

Acknowledgment

Part of the present work is done under the auspices of the doctoral program in Economic Informatics – the doctoral school of Bucharest University of Economic Studies.



Ioan DRAGAN has graduated the Faculty of Cybernetics, Statistics and Economic Informatics in 2011 and IT&C Security Master in 2013. Currently he is a PhD candidate at Economic Informatics ASE Bucharest.