International Journal of Information Management 55 (2020) 102166

Contents lists available at ScienceDirect

International Journal of Information Management

journal homepage: www.elsevier.com/locate/ijinfomgt

Opinion Paper

WHO led the digital transformation of your company? A reflection of IT related challenges during the pandemic

Savvas Papagiannidis[a,*], Jonathan Harris[b], David Morton[b]

[a] Newcastle University Business School, United Kingdom
[b] ICT Industry, United Kingdom

ARTICLE INFO

Keywords:
IT management
Business continuity
Business resilience
Disaster recovery
Digital transformation
Pandemic
COVID-19

ABSTRACT

In this paper we reflect on a number of IT related challenges during the COVID19 pandemic, primarily from a CIO and IT professionals perspective. We consider three time periods, namely the period before the pandemic, the response to the pandemic and the period after it. For each period we discuss the key challenges that practitioners faced and outline important areas to consider for the future. Hopefully, the lessons learnt and the experiences gained will positively inform future academic research and practice.

1. Introduction

The COVID-19 pandemic is arguably one of the most defining crises our societies have experienced in the past 50 years, both in terms of the global reach, but also its impact on numerous levels. In a very short time SARS-CoV-2 has created havoc across continents, effectively halting social and economic activities. In such unprecedent times individuals, and private and public organisations had to respond with unprecedented measures that had a similarly unprecedented impact. Even if a vaccine was to be developed and produced in the short term, the coronavirus scars would be deeply felt for a long time. On one hand the recovery from the loss of family and friends and the impact of the lockdowns is likely to last for a few years at least. On the other, the fear of a recurring pandemic or even of a new one is likely to result in permanent measures and contingencies to prevent such an eventuality in the future.

In such a context information and communication technologies had a vital role to play. Social distancing meant that online applications became critical in ensuring continuity of personal and business services. An online meme asking "*who led the digital transformation of your company*" having COVID-19 as the chosen answer perfectly captures the urgency with which existing digital services were extended and new ones were rolled out, often in haste. IT managers had to react quickly to a rapidly escalating crisis and come up with innovative solutions to ensure business continuity. As Davison (Davison, 2020) put it: "*while disruptions are undoubtedly inconvenient, not to mention potentially life-threatening, they do offer us an opportunity for transformative change*".

In this paper we touch on key IT-related challenges faced by practitioners and reflect on the experience of responding to them, considering that it is not a case of whether a pandemic may happen again, but a matter of when it will happen. COVID -19 is the first significant pandemic in the digital age and this presents a learning opportunity in order to be more prepared for future pandemics, or indeed a reoccurrence of COVID-19 after the easing of lockdown. The paper is organised in three sections, covering the period before the pandemic, the response to the pandemic and the period after it.

2. The period before the pandemic

2.1. ICT risk management and business continuity

Good practice dictates that an organisation's directors need to have risk management processes in place and maintain a risk register that is reviewed regularly. Organisational and IT risk registers identify and describe the risks, and the mitigation strategies. Risk registers also help assess the impact and likelihood of risks, to produce a score and or perhaps use an RAG (Red, Amber or Green) rating. Although such risk registers need to consider both internal/external and micro/macro events one may ask how feasible and pragmatic it was for many organisations to have been explicitly prepared for a pandemic, especially from an ICT perspective. One of the greatest risks in risk management is missing a risk. Even if one register did capture it, how aligned were the

[*] Corresponding author.
E-mail addresses: savvas.papagiannidis@ncl.ac.uk (S. Papagiannidis), jonathan.harris@live.co.uk (J. Harris), dm@itsw.co (D. Morton).

https://doi.org/10.1016/j.ijinfomgt.2020.102166
Received 29 May 2020; Accepted 29 May 2020
Available online 06 June 2020

corporate and IT risk registers and how defined was the IT response to the pandemic? Arguably not many smaller organisations in the private or 3rd sector would have been prepared for such an event. Large organisations may have been more prepared in principle, as the formality and maturity of the risk management process typically depends on the size of the organisation, as well as to an extent on regulatory requirements. Risk management events and planning for events that happen very seldom creates overheads that are often considered a luxury. Funding stresses and other priorities may mean that even if risk management processes had been rigorously followed, the pandemic risk would have probably been underestimated in terms of probability, impact and proximity. Even in cases where the risk of a pandemic was included on the risk register, such inclusion would still be seen as an external event, rather than as something that could affect internal operations, e.g. should members of staff not be able to work due to illness, isolation, or government advice. CIO and IT managers would have to first ensure the continuity of their teams, as such continuity is critical to ensure the wider continuity of the organisation. To this end, business continuity, which is concerned with "*identifying and managing the risks which threaten to disrupt essential processes and associated services, mitigating the effects of these risks, and ensuring that recovery of a process or service is achievable without significant disruption to the enterprise*" (Gibb & Buchanan, 2006), and disaster recovery plans would primarily focus on providing alternative workspaces to comply with social distancing requirements or restoring stressed/failed IT systems. Still how feasible and realistic would it have been to expect plans to have an entire organisation working remotely overnight and for a prolonged period of time? Looking at previous cases of major incidents may offer some insights, albeit localised on a specific industry or geographies. For example, requirements placed on financial services organisations following the 2008 financial crash include the need to maintain excess capacity in call centres and IT systems. The rationale for this is to ensure that they can handle a "run on the bank", where several times the usual number of withdrawals or enquiries need to be handled. Other organisations such as many bricks and clicks retailers did not have the ability to support a massive increase in online ordering as numerous press reports testify (Chancellor of the Exchequer, 2008).

2.2. Mature IT strategies can be effective in a pandemic, even when not designed for one

Technology advances rapidly and over the past few years cloud-based enterprise software applications, hardware and services have become widely available. As such, from a technological perspective, we were in a potentially better position than we would have been, for instance, had the 2003 first SARS pandemic escalated or even if the current one had taken place only 5 years ago. Of course, availability of technology by itself does not translate into good practice. It is an enabler, but not necessarily the main driving force. For example, many users had to transfer both basic and advanced hardware equipment from work to their homes during the lockdowns, so that they could continue working. Still without appropriate connectivity and sufficient knowledge to set them up, many would have struggled. In fact, COVID-19 is interesting in that, unlike many other crises, it does not negatively impact on ICT infrastructure directly, but rather the people that use and support the infrastructure. An IT strategy fully aligned with organisational objectives would have been better equipped to deal with COVID-19 than a less mature strategy. For example, advanced automation within a data centre can be more resilient than manual processes. Similarly, contracts that allow bandwidth expansion based on continuous quality of service assessments could enable prioritisation of services during a crisis. Responding to a crisis is then rendered a matter of scaling services accordingly and not adopting drastically different approaches to replace blocked services.

2.3. Digital infrastructure readiness

Although there may not have been any explicit IT preparations for a pandemic, what aided the ability of many organisations to respond was the implicit functionality provided by elements of undergoing digital transformation initiatives. To some degree, we were accidentally prepared. For example, the adoption of enterprise platforms like Office 365, often primarily for the benefit of cost of the licencing model and not needing to retain so many highly skilled staff for complex software such as Exchange servers, meant that online and collaborative tools were already licenced and available. The pandemic encouraged their use, bringing down any prior resistance to change. In effect, given the circumstances, overnight the relative advantage and perceived usefulness of such applications increased to such a degree that all other factors become secondary.

Mobile computing is clearly a critical component of home working and organisations that have already moved to flexible working where all employees use laptops and can work from home will have been better placed to cope in this crisis than less agile organisations. From the networking and telephony side of things, the availability of IP phone systems with soft phones also helped underpin the rapid deployment of home working capabilities. Also, most organisations typically have VPNs deployed during normal operations. Still, what was more important was the scalability of the VPN solution and the bandwidth to the host data centre. Similarly Citrix/Terminal services/VDI – VDI – where desktops and corporate applications could be published over the web and accessed from laptops, home desktops or tablets made it possible to seamlessly connect users to their familiar corporate applications. The original use cases for such technologies were varied and not related to the pandemic, but proved to be very useful. Such applications would not have been possible without the availability of home superfast broadband and 4 G mobile network access, which enabled home working (Jackson, 2020). This is possibly the biggest factor as to why, had this pandemic hit us only a few years ago, many organisations would have struggled to maintain any kind of meaningful operations.

3. Response and the lockdown period

3.1. Responding to the crisis

By the time the severity of the situation in China started becoming apparent and the epidemic escalated to a pandemic, organisations would have had 2 months at best to prepare. Although in retrospect this may appear to be a potentially sufficient time, one needs to remember that on one hand organisations would have to keep operating as usual and at the same time plan for a response that was not clear. Coupled with governments responding in different ways and often sending ambiguous messages, organisations were left with very short times (typically a few days) to operationalise their responses or even define what the new targeted operating model would look like.

Such responses would have seen business continuity plans being invoked by senior management and response teams. Given the speed with which events unfolded one would expect responses to be reactive in nature, as is typical with incident management, and not looking at the crisis holistically. Normal capacity management processes would not have predicted usage change driven by the crisis. In large organisations, teams in which representation of all functions was sought after would have been more effective in handling the emerging crisis, as, for instance, teleworking is not just an ICT infrastructure issue, but touches on human resource management too. The presence of CEOs/executives would have helped speed up decision making. In such a situation staying ahead of the curve can be of critical importance, as it can ensure that decisions are not taken under excessive stress, which may encourage shortcuts. Still, on the other hand, responding to the crisis by effectively insisting on applying the same processes was likely to be counterproductive. Finally, a key aspect of any decisions made during this period is whether they are expected to respond and serve immediate needs or whether solutions can play a wider role. Having a clear focus on the time horizon can help optimise spending and pave the way for returning to business.

3.2. Digital infrastructure resilience

During a crisis it can be sensible to lower priority or even suspend any non-critical infrastructure. Similarly, planned digital infrastructure work can be suspended unless a project can contribute directly to coping with the crisis. In turn, focus and resources can be redeployed to support essential services that are critical to business continuity. With more and more services moving towards the cloud and often with regulatory requirements to maintain over capacity, plus digital transformation strategies already underway, organisations were already preparing to operate from Internet-connected remote points.

Service contracts can be critical when responding. For example, having a flexible corporate license for VPN software can make it possible for new users to be accommodated quickly. Organisations may have also benefited indirectly from vendor practices, for instance unused fibre optic capacity (dark fibre) or the practice of vendors selling 100Mbit/s circuit on a 1Gbit/s. Similarly, licences and laptops would have needed to be procured quickly. Sales of laptops and desktops increased by 40 % in the first three weeks of March in the U.S., while sales of keyboards, PC headset and monitor sales increased 64 %, 134 % and 138 %, respectively (Rexaline, 2020). Organisations would have had to incur a budget overspend, but any such spending would be a point to assess post crisis and not during the crisis. An exception may be large public sector clients, which were less agile and took time to realise that the situation had changed and decision making needed to be streamlined.

The above assume that infrastructure can be scaled up. If it has already reached capacity and a new installation and deployment was necessary this would have likely not been prioritised compared to addressing failures or supporting emergency services.

3.3. IT support

When it came to support there were two main aspects to consider, namely establishing new digital communication channels and setting up users for remote working. In the first instance management had to use existing digital channels to update staff on the unfolding situation, but also to keep in touch with them. Regular emails and video messages aimed to reassure staff, convey the organisational response, and explain the next steps. Senior management messages from private spaces (e.g. one's living room) reflected the seriousness of the situation as the usual corporate facade was not available, which may also give a more personal touch to the message. Management and staff would have used existing and newly licenced/upgraded video conferencing platforms to keep in touch. Although they all work in similar ways they are also different and often not fully integrated with the rest of the enterprise infrastructure. Given that personal video conferencing is widely available most users would not have had major issues using such platforms. One may not claim the same about setting up users for remote working. Users would have had to have appropriate hardware and networking connections to sustain the applications needed. Not surprisingly, increased demands for support would have put a strain on the existing support desks, which would have to use alternative methods to advise staff on the progress of incidents, for example, by putting an update on the first page of the intranet and ensuring that the intranet opened by default on login or when first opening the web browser. On a positive side, remote assistance and support technologies that have been increasingly used over the years could have been a valuable tool in the IT support arsenals.

3.4. Privacy, security and monitoring

Not surprisingly privacy and security were among the top concerns for IT teams. An organisation under stress is always a prime target for social engineering attacks, e.g. password resetting over the phone without verifications, phishing attempts or malware. Google reported stopping 18 million COVID-19 scam emails per day (Tidy, 2020). Tackling such instances would have required the establishment of clear communication links and expectations so that all users would be more vigilant. Training users to recognise threats is among the most effective ways of dealing with such threats. Still, for such training to be effective, it would have needed to be wider in scope than the typical organisational settings demands were. For example, working from home, often with the whole family in lockdown and having to protect private information from being visible to other members of one's family, can be a challenge in its own right. Similarly, although many organisations may be against having a Bring Your Own Device policy, they may have relaxed their stance In order to ensure continuity. In doing so they would have to accept that ensuring that there is sufficient distancing between personal and work data could be a challenge, while they may be exposing themselves to a wide range of security threats. Having robust mobile device management (MDM) processes and software can address some of these concerns. MDM or Enterprise Mobility Management (EMM) should be mandatory for any organisation that accepts or allows BYOD. This is especially true when BYOD policy is to be used for accessing applications beyond the typical ones, namely emails, virtual meetings and business phones calls. On the other hand, under such extreme circumstances one could argue that productivity could increase with BYOD as employees use devices that are ready readily available to them, they like and know how to use.

3.5. Continuing working on site

Whilst there has been significant variations across organisations, those whose operations are primarily office based will have been able to maximise home working, often to 100 %. Many businesses that need staff to work in a physical location and interact directly with customers had to shut down, despite IT operating normally. Most IT work itself can be and is carried out remotely, but some tasks, e.g. in data centres, will need a physical presence. It is worth noting, though, that it only takes a single step of a process to halt the completion of a task. For example, telecoms engineers, who are classified as key workers, still need to go to exchange buildings. Policies, however, may not allow them to enter customer premises and homes, which can have an impact on the whole process.

3.6. Working from home

Working from home may not be a new idea or practice and for many users it could constitute a significant part of their work experience. Still, full time home working and part time home working can be quite different experiences. Those that could work from home would still occasionally travel to meetings and benefit from face to face interaction with colleagues, which could help vary their work experience. For many, though, working from home, especially in full time mode, would have been a new experience. The need for support rather than training would have been more important in such cases. On one hand, simple instructions like how to connect to corporate systems via VPN may have been necessary. On the other, users may have needed support in setting up and improving sub-optimal home spaces never intended to serve such a purpose. Staff should have been advised to carry out a Display Screen Equipment (DSE) assessment and how to undertake such an assessment, which is important when it comes to health and safety. Also, some employees may feel obliged to work long hours to demonstrate that are not slacking when their management cannot see them in the office. Corporate social media platforms accelerated this because of the crisis and this has encouraged staff to make posts and share experiences, not necessarily directly related to work.

Home working policies, where available, should have helped identify who is eligible or even able to work from home and who is not, maximising the former in the current crisis. It should be recognised that not all office jobs can be easily transferred to home working and forcing users to struggle does not only have an impact on their productivity but potentially jeopardises their wellbeing and long term prospects with the organisation. The policy would have also been a starting point for setting expectations as to how employees are expected to perform while working remotely, taking into consideration other policies, e.g. related to IT security and GDPR.

4. The day after the lockdown

COVID-19 is the first significant pandemic in the digital age, but it is unlikely to be the last. Organisations will need to find creative solutions to the new operational norm, which may feature social distancing for many months. At the same time they need also to consider further lockdown periods or even the possibility of a new pandemic. In this last section we consider a few potential issues that will need to be considered.

4.1. Put employee well-being first

Putting employees' and their families' health and safety first should the first priority. Employees keep an organisation going and without them there cannot be any continuity. Similarly, having to worry about their health and that of their families can place immense psychological pressure that is likely to impact on their performance and productivity. Appropriate measures can reassure staff and make them feel valuable, which can only have a positive impact on the organisation. Understanding users' needs and the mechanisms for dealing with the consequences of the incident is crucial to surviving the pandemic (Pan, Cui, & Qian, 2020). Put differently, one approach cannot be effective for all employees. Existing digital inequalities may have been exacerbated by the pandemic and any mitigating actions need to take them into consideration (Beaunoyer, Dupéré, & Guitton, 2020). While organisations plan the gradual return of employees to their offices, they have the challenge of balancing the desire of employees to spend more time working from home than returning to the office. Employees may feel anxious about the risks that this poses to them personally. How such anxieties are managed can have an impact on both individuals and the organisation, not just operationally but also how its culture is shaped going forward.

4.2. Build resilience to ensure continuity

Once the storm calms, from a technology perspective, senior management, IT Directors and CIOs are likely to revisit their business continuity plans and explicitly account for the next pandemic. They may attempt to prepare an "*Information and Communication Technology Pandemic Plan*" that aims to prepare the organisation for such an eventuality. Planning for a pandemic will not be less challenging, if a pandemic was to occur again in the future. Devising specific plans to respond to events that are difficult to predict (either when they will happen or how exactly they will manifest themselves) is not likely to be an effective approach. Instead, organisations may wish to consider how to increase business resilience across the organisation. If one is prepared for a pandemic without overburdening the system, then one is likely to be able to respond to a much wider range of crises.

Business resilience can be defined as the ability of a business to anticipate, prepare for, and respond and adapt to incremental change and sudden disruption in order to survive and prosper (ISO, 2017). IT service continuity and business continuity more broadly should not be seen just as responses to disruptive incidents. Instead, an impact analysis could help identify critical employee groups, business processes, infrastructure and data, external relationships etc and consider how to support and scale up when certain conditions arise. Organisations need to prioritise decisions and investment based on roles and tasks and not hierarchy.

Similarly, it can help identify areas that are not critical and resources can be diverted accordingly. In turn, teams with representatives from all functions will pick and adjust the appropriate parts of the plan as a response. Building resilience in such a manner is likely to be most cost effective. Also, as disruptive incidents of a smaller scale are likely to occur intermittently, the organisation learns to respond and adapt over time, creating an automatic failover culture.

Finally, organisations may also consider, where possible, their ecosystem's resilience. For instance, instead of delaying payments, they could expedite when they can do so, in order to ensure that their suppliers' cash flow is not disrupted. In doing so, not only do they ensure that their immediate relationships survive but also that they are strengthened, which can have a positive spillover effect after the pandemic is over.

4.3. Digital infrastructure and supporting users

Although central ICT infrastructure typically operated as per usual, it was often the more "basic" issue that caused significant disruptions. Users requiring support or not having appropriate and secure hardware were common issues during the lockdown period. Instead, organisations could invest in "resilience-in-a-box" solutions, namely small terminal boxes that are ready to connect securely to the corporate networks remotely. Such devices can be given to employees who may potentially need them when they are inducted. They can be taken home and stored or even used for regular home working, where appropriate. Users would only need to add a monitor, keyboard and mouse and connect to their Wi-Fi. Such tasks are within most users' IT skills and hence will require minimal support. During a discontinuity incident users can use these boxes to connect to the corporate networks. The first time such a connection is established, the boxes can be updated, after which point users can access their applications as usual. Organisations will be able to maintain remote control of the devices and decommission them once an employee leaves them. The above approach can effectively minimise provisions for disaster recovery office space, with savings funding such an alternative setup. It also enables corporate control of the hardware and thus removes some hard to mitigate risks associated with BYOD hardware. Depending on the exact arrangements both needs server-side and licencing adjustments may be necessary to accommodate such a scenario.

4.4. Space and users

The way space is utilised is likely to be reviewed and fundamental changes introduced. In the first instance, organisations are likely to amend/develop their hot desk and meeting room policies in light of the ongoing pandemic risk. Physical office space will still be needed as it is difficult to substitute the benefits that direct engagement between management and employees can have. It will be challenging to recreate such an engagement online without resulting in a "yet-another-video-call". Still, with many users actively demonstrating they could cope even under such extenuating circumstances, one can but ask if more agile and flexible working that is partly mobile or remote is a way forward. On one hand it can bring significant efficiencies, e.g. smaller physical spaces needed, less travel etc. On the other it may contribute to users' employment satisfaction and well-being. It can also open up an opportunity as it can make it possible to recruit talent from across the world. The above does not mean that physical spaces and meetings are not going to be required.

4.5. Productivity and IT

Asking if productivity has been impacted positively/negatively by home working during the pandemic is the wrong question. Instead managers should be asking which lessons during this period can be applied to improving productivity, considering the experience from the forced upon us experiment of remote working. Although such time may not translate to additional work time, not having to commute can mean employees are better rested. Similarly, although online meetings may typically be shorter than offline ones, this may be more of a teleconference fatigue as opposed to users being more productive. Attitudes of managers and employees may have been affected by the lockdown experiences and should be interpreted accordingly.

Acknowledgment

The authors would like to thank the IT professionals who offered valuable feedback on the manuscript and shared their experiences.

References

Beaunoyer, E., Dupéré, S., & Guitton, M. J. (2020). COVID-19 and digital inequalities: Reciprocal impacts and mitigation strategies. *Computers in Human Behavior, 111*, 106424. https://doi.org/10.1016/j.chb.2020.106424.

Chancellor of the Exchequer (2008). *Financial stability and depositor protection: Strengthening the framework.* London.

Davison, R. M. (2020). The transformative potential of disruptions: A viewpoint. *International Journal of Information Management*102149. https://doi.org/10.1016/j.ijinfomgt.2020.102149.

Gibb, F., & Buchanan, S. (2006). A framework for business continuity management. *International Journal of Information Management, 26*(2), 128–141. https://doi.org/10.1016/j.ijinfomgt.2005.11.008.

ISO (2017). *ISO 22316:2017 Security and resilience — Organizational resilience — Principles and attributes.* Retrieved from.

Jackson, M. (2020). *COVID-19 – OECD compare exchange traffic between countries.* Retrieved fromhttps://www.ispreview.co.uk/index.php/2020/04/covid-19-oecd-compare-exchange-traffic-between-countries.html.

Pan, S. L., Cui, M., & Qian, J. (2020). Information resource orchestration during the COVID-19 pandemic: A study of community lockdowns in China. *International Journal of Information Management, 54*, 102143. https://doi.org/10.1016/j.ijinfomgt.2020.102143.

Rexaline, S. (2020) Retrieved from https://finance.yahoo.com/news/webcam-computer-accessory-demand-booms-185122718.html.

Tidy, J. (2020). *Google blocking 18m coronavirus scam emails every day.* Retrieved fromhttps://www.bbc.com/news/technology-52319093.

Prof Papagiannidis is the David Goldman Professor of Innovation and Enterprise at Newcastle University Business School. His research interests revolve around electronic business and its various sub-domains and how digital technologies can transform organisations and societies alike. More specifically, his research aims to inform our understanding of how e-business technologies affect the social and business environment, organisational strategies and business models, and how these are implemented in terms of functional innovations (especially in emarketing and ecommerce). His work puts strong emphasis on innovation, new value creation and exploitation of entrepreneurial opportunities, within the context of different industries. Apart from the impact that the Internet and related technologies can have on businesses, he is also very much interested in the impact such technologies can have on individual users.

Jonathan Harris has over 25 years of experience working in the ICT industry, holding a number of senior positions including IT Director for a multi-national support services company and IT Programme Director for a FTSE100 PLC. Jonathan currently manages the Connecting Cumbria superfast broadband programme, which aims to provide a minimum of 24Mbps download speeds in areas of the county that will not be covered commercially and which are typically rural, or increasingly deeply rural in nature. Jonathan also has a broader digital infrastructure role within Cumbria County Council, including acting as technical lead for the Digital Borderlands initiative as well 4 G and 5 G mobile technology.

David is an interim IT Director and Consultant. He is a technology enthusiast, active in the IT industry for over 35 years. He advises on IT strategy and business change for a wide range of types and size of organisation.