SEPTEMBER 2021

BEYOND THE DIGITAL STATUS QUO

Experiences and Lessons from the COVID-19 Pandemic

RICHARD MCDONALD, MICHAEL POWER, ARON FEUER & JULIAN BOTHAM

PUBLIC POLICY FORUM
FORUM DES POLITIQUES PUBLIQUES
PPF

TABLE OF CONTENTS

PUBLIC POLICY FORUM
FORUM DES POLITIQUES PUBLIQUES

PPF

ABOUT PPF

Good Policy. Better Canada. The Public Policy Forum builds bridges among diverse participants in the policy-making process and gives them a platform to examine issues, offer new perspectives and feed fresh ideas into critical policy discussions. We believe good policy is critical to making a better Canada—a country that's cohesive, prosperous and secure. We contribute by:

- Conducting research on critical issues
- Convening candid dialogues on research subjects
- Recognizing exceptional leaders

Our approach—called **Inclusion to Conclusion**—brings emerging and established voices to policy conversations, which informs conclusions that identify obstacles to success and pathways forward. PPF is an independent, non-partisan charity whose members are a diverse group of private, public and non-profit organizations.

1400 - 130 Albert Street
Ottawa, ON, Canada, K1P 5G4
613.238.7858

ppforum.ca @ppforumca

ISBN: 978-1-77452-088-8

WITH THANKS TO OUR PARTNERS

amazon web services institute

VALENCIA
INFORMATION & INFRASTRUCTURE PROTECTION

PROCESS

To prepare this report, the authors:

- Reviewed industry publications concerning digital transformation, the COVID-19 pandemic, remote work and related topics, restricting the search to those published in late 2019 or after;
- Interviewed 15 senior executives from a cross-section of Canadian public and private sector organizations including federal, provincial and municipal levels of government; and
- Hosted a roundtable with a larger selection of senior executives.

The interviews and roundtable operated under the Chatham House Rule; therefore, remarks are not attributed to individuals.

Disclaimer: The Public Policy Forum and the authors would like to recognize and thank Amazon Web Services for their sponsorship of this important piece of work. The content of this paper, including any errors, is the responsibility of the authors listed below.

ABOUT THE AUTHORS

Richard McDonald provides consulting services focused on Strategy and Cyber Security, after retiring from the role of Chief Information Officer of the Canadian Security Intelligence Service.

His 42-year career has included 18 years in government, 17 of which were in the classified Security and Intelligence community, in positions from Director to ADM level and in roles such as Chief Information Officer, strategy, architecture, IT security, information management, and information technology. He has also led innovation programs, mentoring programs and staff development initiatives. Prior to government, Richard worked for 23 years in the Nortel family of companies, in technology strategy, product management (including a two-year international assignment in Japan), security, IT management and software development.

Richard holds an MBA, Master's and Bachelor's degrees in Computer Science, certificates in Photography and Graphic Design, and is a certified Lean Six Sigma Black Belt.

Michael Power is a recognized expert in privacy. He is the author of The Law of Privacy, published by Lexis Nexis, as well as Halsbury's Laws of Canada – Access to Information and Privacy (2005, 2011 and 2016 editions), published by Butterworth's. Michael has over 15 years' experience dealing with privacy-related

questions. His past experience includes serving as a member of the federal Department of Justice, a partner at a national law firm and as Vice-President, Privacy and Security at an Ontario Crown Agency.

Aron Feuer is a recognized expert in cybersecurity. In 1998, he founded Cygnos Information Security, a national consultancy acquired by a national accounting firm in 2012. Aron has extensive industry experience across all three levels of government, finance, technology and healthcare. His project experience includes leading the IT Forensics investigation in the Robocall scandal, incident response to attacks by the hacker group Anonymous and the security certification of Canada's classified networks. Aron is the head of Algonquin College's cybersecurity program advisory board. He is currently co-authoring Privacy Fundamentals for Canadian Practitioners with the International Association of Privacy Professionals.

Julian Botham works as a Junior Penetration Tester for Valencia IIP. Prior to working with Valencia, he was part of the Bell Public Safety Group and helped deliver CAD software systems across Canada and the US to fire, EMS and law enforcement departments. While with Public Safety Group, Julian provided QA, IT support and developed a knowledge base for their proprietary software. Julian continues learning through online courses and certification programs after completing his Cyber Security Analysis diploma at Willis College.

EXECUTIVE SUMMARY

The COVID-19 pandemic has proven to be a test of the value of cloud-based services and digital transformation. This includes various factors that were slowing their adoption, such as legacy processes, practices, policies and, in some instances, financial structures. When considering the spectrum of digital transformation, organizations should create corporate architectures that meet their requirements and constraints. They should also recognize the time needed to do so.

Organizations that had successfully adopted digital transformation were able to better respond to the pandemic, to a degree proportional to the depth of their transformation. The pandemic demonstrated that ensuring an "untethered" workforce allows an organization to change *how* they work. Mobile-enabled workforces were able to quickly resume operations while organizations that had rearchitected their systems using modern digital approaches, often cloud-based, were able to quickly modify existing services and deploy new ones. Remote work has shown short-term benefits to employees, and many prefer it; however, there appear to be undesirable long-term effects on the culture of organizations and their ability to innovate.

Organizations wanting more technological agility should recognize that digital transformation is not a destination but a journey along a spectrum that moves from simple to complex. Using cloud-based services does not necessarily mean being digitally transformed. The transformation of business processes, allowing change in not only *how* but also in *what* an organization does, is not a short process.

Moving to a different post-pandemic environment, especially as organizations consider a hybrid-model of remote and in-office work, will require a greater emphasis placed on security and privacy. Employee training will help but organizations will also need to develop modern, relevant, standard configurations and practices for working remotely, including computing and physical infrastructure. Associated with this is a need to review the streamlined or temporary measures used to implement emergency services and ensure appropriate risk-management decisions are approved and recorded.

Public sector IT leaders have been both responsive and adaptive in navigating the challenges that arose during the pandemic crisis. The challenge will be in taking the digital transformation lessons, learned as they reacted to the pandemic, and applying them as Canada moves into a "post-pandemic" world.

INTRODUCTION

In 2019, the Public Policy Forum (PPF) published a paper titled The Risk of the Digital Status Quo: How Governments Can Enable Digital Transformation, asking a fundamental question:

> **"Since it is generally accepted that migrating enterprises to cloud-based services brings multiple benefits, why is migration proceeding slowly or, in some cases, not at all?"**

The Risk of the Digital Status Quo argued that the status quo is *not* a low-risk alternative for public sector organizations. If an organization compares the risks associated with cloud migration to the risk of doing nothing, and assumes the latter risk is very low, it will erroneously conclude that staying with the status quo is preferable.

This paper was originally planned to be a review and update of the reaction to that thesis and the continuing evolution toward cloud-based services. Then, the pandemic happened.

The COVID-19 pandemic has been a crisis that mobilized organizations and economies – one that tested both the operational assumptions and preparedness of every public sector organization in Canada. Given the adage, "never let a good crisis go to waste", this paper takes the opportunity to consider digital transformation in the time of pandemic and to offer recommendations to organizations as they consider how best to approach digital transformation, security, and workers, post-pandemic.

COVID-19: A TEST FOR DIGITAL TRANSFORMATION

The COVID-19 pandemic has served as a massive experiment, testing the thesis of the 2019 paper. "Doing nothing" became a greater risk than using new technology, much of which already existed and simply had not been adopted.[1] One government executive interviewed for this paper called the pandemic a "forcing function", which "took the option of doing nothing off the table."

However, the bias towards the "status quo" when assessing risk is not a complete explanation of slow movement toward digital transformation. Many policies and regulations also served as substantial barriers to rapid response. Some organizations enabled their crisis response by using available emergency authorities to streamline, reinterpret, or even circumvent problematic policies. Other organizations, though, found workarounds that allowed services to continue functioning but were contrary to formal policies and protocols, such as the tacit approval of the use of unapproved sharing services or connectivity methods to enable emergency remote work.

THE TRANSFORMATION SPECTRUM

The subject of *The Risk of the Digital Status Quo* was *cloud adoption*. However, in reviewing case studies and interviewing stakeholders, ease of transformation involved not only cloud adoption, but also other interrelated factors, such as *remote work*, *digital transformation,* and *agile development*.

The pandemic has proven the thesis of *The Risk of the Digital Status Quo* correct but incomplete. Legacy systems have been difficult to pivot or repurpose quickly. Many contain lingering security vulnerabilities because they are beyond the vendor's support period for security patches for vulnerabilities, which became more critical when the applications were deployed to the more accessible online environment. On the other hand, organizations that had undergone significant digital transformation before the pandemic, especially if they became cloud-based, were generally able to respond to the crisis by rapidly changing existing services or deploying new ones.

TRANSFORMATION VS. CLOUD MIGRATION

As a starting point, it is important to acknowledge that "digital transformation" and "cloud migration" do not mean the same thing and each is possible without the other. However, these terms were often used interchangeably in interviews conducted and case studies read. One service provider interviewed noted that "digital transformation is an *outcome*, while cloud adoption is a *means* to that outcome."

It is possible to be wholly *cloud-based*, but not be *digitally transformed*. This would be the case if an organization "lifted and shifted" all legacy applications from an on-premises data centre to a virtual data centre running as cloud-based "infrastructure as a service". The organization would realize several benefits, but the systems would still be, by definition, the original legacy systems. The organization might have transformed *how it runs its IT department*, but it will not have transformed its *business*.

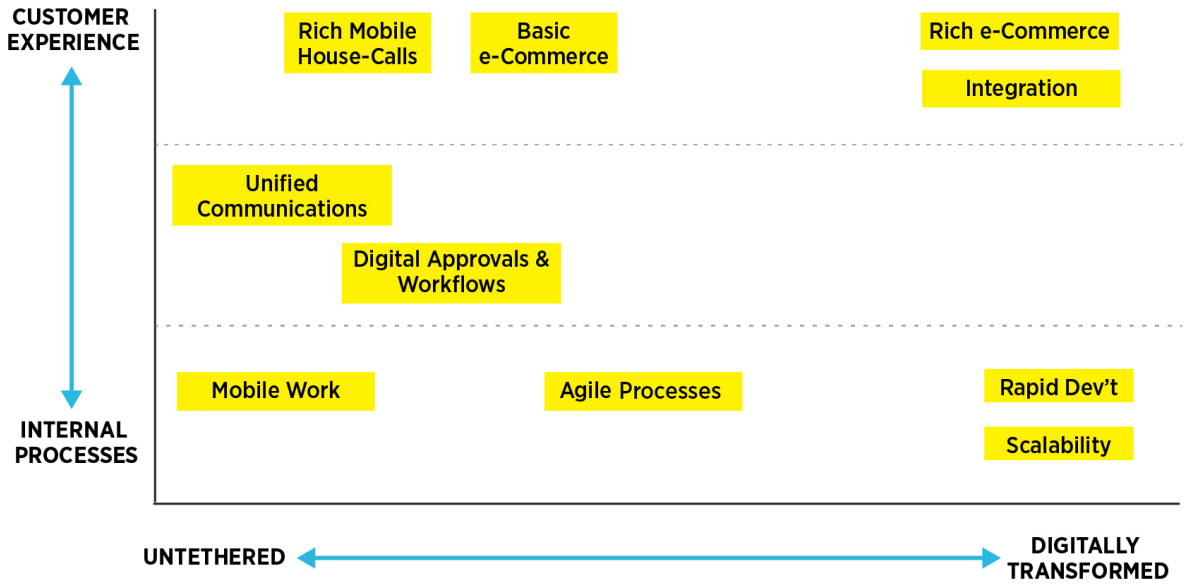
Organizations can also be *digitally transformed* without being *cloud-based*. One organization interviewed is in this state: they recognized the need for modernization but feel prevented from migrating to the cloud by policy and financial constraints. They have re-architected their IT systems to include modern service-oriented architectures, standardized application interconnections, and browser-based user interfaces rather than dedicated client applications. They consider themselves "digitally transformed", while using on-premises equipment. One would expect that organizations digitally transformed in this way would be able to move to the cloud more easily in the future, since the challenging work of re-architecting applications is already done.

In most cases, however, cloud migration facilitates digital transformation. It has been called "central to a developed technology strategy."[2]

COMPONENTS OF THE TRANSFORMATION SPECTRUM

While transformation towards modern digital platforms was key to rapidly adapting to the pandemic, this statement is simplistic and one must ask, "what *kind* of transformation?" It is important to note that this is not a binary choice; it is not a case that "one is transformed, or one is not". As detailed in Figure 1 below, transformation is a *spectrum* of changes to business processes, ranging from simple to complex.

Figure 1: Common outcomes of transformation



UNTETHERED

"Untethered"[3] organizations have decoupled the ability of employees to work from their physical location.[4] Organizations untether through *mobility capability:* ensuring all employees *can* work away from their desks, even if they do not actually do so. This means preferring laptops over desktops and cellular phones over landlines, as well as ensuring that effective remote access will allow essential applications to be reached and used from anywhere. In using remotely accessed (usually cloud-based) office communication tools—such as email, chat and conferencing for routine communication tasks —there is no difference between sitting at a desk in the office or using an Internet-connected laptop outside the office.[5]

Transformation that stops at the "untethered" phase tends to be inward facing, affecting services used by employees but not by customers. Products and large-scale business processes are not substantially changed.

Thus, being untethered allows a rapid change in *how* one works but not in what one *does*.

DIGITALLY TRANSFORMED

On the other end of the spectrum, "digitally transformed" organizations have made changes that allow new business functions to be added, or existing functions to be dramatically changed, very rapidly. Where being

untethered allows an organization to rapidly change *how* work is performed, digital transformation allows an organization to rapidly change *what work it does*.

Organizations that have achieved this are able to rapidly:

Reduce or increase scale of operations

Modify existing business offerings and processes

Develop new business offerings and processes

Digital transformation can affect "outward-facing" services used or seen by customers, as well as corporate services used by employees. It is enabled by modern multi-layer, service-oriented system architecture, services integrated through well-defined interfaces, and modern development processes. Although this can be achieved without using cloud-based services, most modern transformation is cloud-based, which couples the modernization of proprietary business processes with the use of third-party cloud services.

SPEED AND OUTCOME

It is easy to prioritize and implement untethering in response to a crisis, but digital transformation, which has a more profound impact, is a multi-year effort that cannot easily be rushed. Untethering has been called the "low-hanging fruit," subject to a caution that an organization will eventually run out of easily "migratable" services.[6]

In a 2020 survey of small businesses using cloud services, about 70 percent had achieved what can be characterized as untethering, while only about 30 percent had achieved digital transformation.[7] This is consistent with the interviews conducted for this paper: each of the individuals interviewed said their organization had achieved at least untethering and listed the benefits of doing so, while only a few had achieved digital transformation but credited it with more substantial benefits, such as being able to deploy new services, in response to the pandemic, very rapidly.

At the outset of the public health crisis, most organizations already had—or were able to quickly implement—untethering and benefited from the ability of staff to work remotely through lockdowns and reduced office capacity. Organizations that were already digitally transformed benefited by being able to quickly adapt their business processes or develop new ones, while organizations that were not already digitally transformed may have accelerated their transformation programs.[8] However, at this stage of the pandemic response, there are no reports of substantial benefits from recently launched or accelerated transformation programs.

The lesson from these experiences seems clear: strategic investment works, but it needs to start early. When a need becomes an emergency, smaller, shorter-focus investments are required, providing smaller returns more rapidly.

LESSONS FROM THE PANDEMIC

Many models indicate that crisis response activities proceed through recognizable phases. One interviewee used a three-phase model to describe their organization's pandemic response: Reaction, Response and Recovery.

Reaction, as an unplanned phase, refers to procuring anything thought to be needed and granting exceptions to use available non-standard services. A transition to emergency analogs of basic services happened rapidly (e.g. moving most meetings to cloud-based services, such as Zoom). The immediate challenge was resource availability. One interviewee provided the example of the federal government's lack of licenses and bandwidth for the sudden surge in demand for remote access services, resulting in employees being scheduled to access remote services at different times of the day.

The *Response* phase sees the beginning of more planned deployment of services, resulting in the development of new work cadences. This may be characterized as the phase of "getting the business running in the new situation". For example, remote access and other services stabilized at the required capacity and business processes were adjusted to accommodate electronic approvals and remote consultations.

In the *Recovery* phase, organizations planned new services, developing or procuring the tools necessary for implementation. Clients were offered new ways to access existing products and services, and new services were developed and deployed.

OBSERVATIONS AND LESSONS LEARNED

The following observations and lessons can be drawn from the interviews and research conducted for this paper.

Organizations Can Move Much Faster Than They Think

Organizations learned they could move much faster than they thought; Microsoft's CEO Satya Nadella famously called the experience "two years of progress in two months".[9] Studies have shown organizations changing or developing services 20 to 40 times faster during the pandemic when compared to their usual

performance.[10, 11] This is consistent with the remarks of several interviewees who indicated their previous appetite for risk had probably been too low.[12]

Many organizations that were not transformed to any degree began or accelerated transformation programs. Untethering was achieved but, in most cases, not full-scale digital transformation, which is a long-term endeavour. Untethering brought advantages and left organizations better positioned for further transformation. Cloud-based communication services have been called the "unsung hero" in the pandemic response.[13]

Having proven feasible at a larger scale and for a longer period than ever before, remote work has been credited with numerous benefits and is expected to be "here to stay" after the pandemic.[14] But the news is not all positive; we discuss, below, some concerns that are emerging regarding the effects of remote work on culture.

Digital Transformation Drove Agility

The COVID-19 crisis has been called an "accelerant of trends already underway".[15] Organizations that were digitally transformed before the pandemic fared much better. They were able to rapidly move to new business models and scale to new demand.[16, 17] Some risk-taking was necessary to achieve this, but the risks were manageable and lower than the impact of being unable to pivot.

Digital transformation facilitated a successful reaction to the pandemic and organizations with established Agile methods,[18] especially with supportive processes up-and down-stream from development, also fared better.

The example cited by many reports and interviewees was Government of Canada's implementation of CERB, the Canada Emergency Response Benefit. CERB was deployed in a few weeks—much faster than typical government programs—and the ability to develop and deploy so rapidly is credited to the fact that the development team was untethered, accustomed to working remotely, well-versed in Agile methods, and used a cloud-based development environment.

A significant factor in accelerating delivery was "loosening the reins on Agile". Many organizations had already adopted Agile development and had teams that were both ready and able to deliver quickly. However, the ability to do so was impeded by legacy governance processes. When these constraints were softened, rapid development and release was possible.

While reflecting longstanding pre-COVID-19 corporate culture, organizations recognized that at least some of those constraints existed to ensure a level of quality, compliance and assurance. Although no significant examples were reported, it seems likely that there will be some failures or reversals resulting from

accelerated development in the future and it may be necessary to revisit the subject of constraints to better calibrate governance and risk tolerance.

In addressing and softening constraints, one idea raised in the roundtable group was the concept of "one-way doors" and "two-way doors" —some decisions can easily be reversed if they turn out to be errors (two-way doors), while some cannot be easily reversed (one-way doors). Decisions that would be difficult to reverse, such as the choice of an Enterprise Resource Planning (ERP) package, warrant more pre-decision oversight; but easily reversable decisions, such as selecting one of many alternatives for a user interface design, are a good place to use a "try it and see" approach. Agile encourages identifying "two-way doors" — lightweight, low-impact opportunities to test experimental decisions—where possible.

Many of the business "pivots" in response to the pandemic, were seen as "two-way doors": it was worth trying a new approach to delivering service (e.g. curbside pickup) and there was little to lose if it proved unsuccessful.

The Value of Cloud-Based Services: Cost Transparency, Scalability and More

Cloud-based systems support more transparent and complete investment decisions. While there are cost savings to be had, especially in the elimination of surplus IT capacity acquired to address peaks in demand, costs for cloud-based services can *appear* to be higher since hosting services in the cloud makes the total cost of ownership clearly visible. In contrast, traditional on-premises capital investment often fails to account for, or misattributes, some costs of ownership, resulting in a perception of lower cost overall.[19] The true cost of ownership represented by cloud expenses promotes better-informed business decision making.

The true benefit of cloud, however, has proven to be its *agility*: its ability to scale rapidly and its ability to support rapidly developing new services or changing existing ones.

Scaling up has been clearly demonstrated. The Canadian Digital Service notification system quickly accommodated a 100-fold increase in transaction volume and a Canadian health network accommodated a 10-fold increase in the number of patient video visits.[20]

The use of cloud-based services in providing an ability to scale *down* will also be an asset as the economy recovers from the pandemic. As the volume of emergency services and special circumstances reduces, cloud-based systems can scale back with a corresponding reduction in service costs. There is no burden of fixed capital cost that remains whether the systems are used or not.[21]

Even the ability to scale rapidly is not the complete story on the advantage of cloud transformation. As one senior executive interviewed said, **"The big contribution of cloud is beyond the scalability: it's the easy access to and integration of advanced services that would be challenging to build, or**

unaffordable, on-premises." The ability to construct new service offerings is enabled by rapidly combining components built in-house or acquired from other cloud users.

Successfully Adapting Organizations Developed a Different Approach to Risk

The Risk of the Digital Status Quo characterized organizational approaches to risk assessment as flawed because they incorrectly assumed that risk was always associated with change and that the risk of *not changing* was low or zero.

In the development of new policies, programs and systems, the traditional approach to risk management was heavily geared to risk *prevention*: investing up front in critical review, challenge, oversight and gating processes, to reduce the likelihood of failure upon implementation.

Organizations that successfully adapted to the pandemic used a different approach. They correctly compared the risk of a proposed development to the risk, to business or society, of *not* doing the proposed development. While some interviewees used phrases such as "raising our risk tolerance", others argued that what had really occurred were *better-informed* risk decisions. At the time of this paper's publication, it is too early to predict whether increased risk tolerance will continue post-pandemic, or whether there will be a return to what *The Risk of the Digital Status Quo* referred to as an "ingrained risk aversion among Canadian public servants".[22]

The frequently cited example, again, was CERB. To deploy quickly, it was necessary to fast-track, or even set aside, certain oversight tasks traditionally used to avoid risk. Since the economic risk of delaying CERB payments to Canadians was deemed higher than the economic risk of fraud or error, there was a conscious decision to forgo the usually "front-heavy" risk avoidance processes and a focus on expedited delivery of benefit payments followed by post-payment controls.[23]

These are not new observations. It has long been understood that mature risk-taking is related to, and essential for, Agile development. In the roundtable discussion, this idea was both pronounced and repeated. Organizations remained focused on rapid delivery with pronouncements such as, "perfect is cancelled" and "good enough is more than enough".

> **One participant put it as, "we moved from *project*-focused (managing by monitoring compliance to a process) to *product*-focused (managing by monitoring progress towards a desired outcome)".**

The Importance of Adaptive Leadership

In many organizations, business continuity planning (BCP) is done in silos and does not provide a sufficiently integrated response to an event which affects the entire organization.[24] Furthermore, the traditional risk-based prioritization used in planning tends to emphasize events with moderate to high likelihood and impact. Events with "very low likelihood but very high impact", such as a global pandemic, may not be prioritized for further planning.[25] For example, several interviewees made comments to the effect, "this was unlike our BCP exercise"—few had BCPs designed for a duration of more than a year.

Through research, interviews and the roundtable, it was made clear that many organizations were making decisions to take certain risks to keep specific business functions running, either to stay in business or to supply essential services.

In some cases, policies and regulations contained emergency provisions that allow for a deviation from standard requirements during a crisis. Also provided were examples of organizations where staff undertook measures deemed necessary but contrary to documented policy or standards. This risk-taking was often with the full awareness and "tacit approval" of senior management, but without written record. The result is that individuals acting in good faith may be taking *personal* risk if the actions are outside policy and no exemption is documented.

The pandemic response provides a good basis to distill those leadership attributes associated with the successful navigation of a crisis:

- ➔ **Take quick, firm, definitive action, even if it is unpopular;[26,27]**
- ➔ **Act based on data and, as the data changes, legitimize reversal and revise plans;**
- ➔ **Use the concept of "one-way doors" and "two-way doors" to apply more risk scrutiny to decisions that cannot easily be reversed or recovered from if incorrect; and,**
- ➔ **Use available authorities to take measured, well-informed, risk decisions and take accountability for their outcomes.**

SECURITY AND PRIVACY

The pandemic forced a re-examination of security and privacy policies and practices .

SECURITY

The special conditions under which people are working during the pandemic have proven to be fertile ground for security attacks.[28] Experts interviewed for this paper emphasized that exceptions were made to permit full untethering. At a time when attacks are increasing, our ability to make measured judgements about cybersecurity and social engineering attacks is compromised. The Canadian Centre for Cyber Security calls for attention to this matter: "We expect the remote workforce almost certainly to be increasingly targeted by foreign intelligence services and cybercriminals."

Social engineering attacks have been more prevalent and more successful during this crisis, with one study showing a 350 percent increase in phishing attempts.[29] Such attempts, when successful, are a common cause —if not *the* most common cause —of security breaches.

Similarly, there has been a large increase in *ransomware* attacks since, during a health crisis, healthcare organizations are attractive targets for such extortion.[30] In 2020, almost 25 percent of the ransomware victims in the U.S. were healthcare providers and half of all healthcare security breaches are now ransomware.[31]

The need to rapidly transition employees to remote untether work has left organizations open to security risks. As one interviewee noted, "it was surreal to be discussing security with the security team over an unsecured video link". What organizations will now need to consider over the long-term—since a likely hybrid model of untethered work remains —is the need to review security practices, revise risk acceptability criteria and outline employee training.

PRIVACY

One initial line of research for this paper was a concern about privacy and whether it received insufficient attention as organizations dealt with the COVID-19 crisis. This does not seem to have been the case.

All the organizations interviewed indicated that attention to privacy was not diminished while reacting to the pandemic. In some cases, streamlined privacy assurance methods, such as checklists, in place of full Privacy Impact Assessments, were used, with appropriate approval.

HUMAN CAPITAL ISSUES

The effect of the pandemic on human capital, especially the effects on the staff implementing and operating the systems that were developed or changed in response, was a topic that frequently arose in the course of interviews for this paper. These human capital issues fell into four categories:

Skill sets

Issues with remote work

Employee health and well-being

The cycle of recruiting, onboarding, retention, and attrition

SKILL SETS

When asked whether their organizations had the skills needed to respond to the new operating conditions of the pandemic, senior managers responded consistently, both in interviews and in the roundtable workshop, that their IT department staff had the skills needed to rapidly change or deploy new services in a digitally transformed environment. If anything, according to some leaders, some staff had previously been frustrated at the lack of opportunity to use their skills and training.

When, out of necessity, legacy constraints that impeded modern development methods were relaxed, these staff were able to work at a pace not previously seen.

HUMAN RESOURCES RECRUITING AND RETENTION

Executives interviewed for this paper generally reported that remote work was having a positive effect on recruiting. “Work from home” really means “work from anywhere” and many organizations are taking advantage of this ability to recruit people who live at a distance and offer them work without the need to relocate. One executive remarked that the broader recruiting facilitated by remote work appears to be improving diversity in their workplace.

However, it was noted that onboarding, training and cultural assimilation were harder. Even recruiting did not always benefit. Some managers hiring highly specialized staff, such as data scientists, rely on in-person interviews and team visits as part of their selection process, and find wholly remote interviews to be less effective.

Those interviewed indicated that to-date there has been no increase in attrition. Several interviewees suggested that this is temporary: that people are reluctant to change jobs during this uncertain economic time, and an increase in attrition may follow when the perceived economic risk has reduced.

WHAT IS HOLDING THE TRANSFORMATION BACK?

Despite the positive results realized by many organizations, others are still struggling with the decision to embark on the journey toward digital transformation, or struggling to obtain funding, approval and priority for that journey.

FUNDING STRUCTURE AND MODEL

How funding is obtained, managed and structured in organizations can be an unintended disincentive to migrating to cloud-based services.

Legacy environments are expensive liabilities. One interviewee complained, "It's easy to say 'Cloud First' as a vision, but we have a large base of on-premises legacy equipment whose upkeep is consuming a lot of our available funding and resources. We need to find a way to break this cycle."

Funding allocation in organizations is often tied to organizational silos. One CIO interviewed explained, "Infrastructure costs, such as power and cooling, are built-in to the price I pay for cloud services. But, when we build in-house, power and cooling are in the Facilities department's budget, not mine. So, for my on-premises systems, power and cooling appear, to my budget, to be *free*". Thus, it may appear to departments, from a budgeting perspective, that on-premises infrastructure is less expensive.

The fact that cloud adoption tends to move the upfront purchasing of IT infrastructure, software and services to a recurring subscription-style model is generally considered an advantage. However, this is not necessarily the case for everyone. As noted by an executive in one jurisdiction, departmental budgets for upfront costs are often allocated through a straightforward process. However, being able to bill a recurring expense, in his organization, generally requires a taxation increase, which no one wants to be associated with.

The "all-in" pricing of cloud makes the costs of maintaining data centers clearly visible, which should result in better-informed decision making. However, if such costs are compared to infrastructure funding alternatives where the total cost of ownership has *not* been factored in (as commonly occurs), cloud services may appear considerably more expensive; therefore, not an acceptable option.

Finally, the ease of procuring additional capacity or services on the cloud concerns financial comptrollers since it may make unplanned expenditures easier. This concern about potential cost escalation can be addressed with governance and cost management systems, but is often overlooked when organizations first move to cloud.

LEGACY PROCESSES

Interviewees provided numerous examples where legacy processes in organizations were impediments to digital transformation:

- Governance processes — both up - and down-stream from IT —may impede the use of Agile processes for rapid development. Examples, based on obsolete waterfall development cycles, included security assessment processes (build the system, then assess its security) and procurement processes (specify everything needed, compete, and procure once, up front).
- Outdated approaches to change impede responsiveness. Cloud-based systems change incrementally and frequently. Burdensome change management processes, developed when change was a yearly event, can be overwhelmed when change is daily. Security policies requiring re-accreditation of a system when it changes both impede the use of frequently-updated cloud-based solutions and act as a disincentive to patching systems – an ironic outcome for a security policy.

"NEW NORMAL" CONCERNS

At the end of each interview for this paper, interviewees were asked what they thought the post-pandemic workplace would be like, as we return to some kind of "new normal". The answers were wide-ranging, but common themes arose.

Among organizations that achieved major pivots to new business models or new services, a common comment was:

> **"To achieve this response, many legacy practices were modified or streamlined. Some of this was necessary risk-taking, but some was simply updating old practices that were obsolete or too risk averse. After the crisis passes, we need to review what was achieved, and what was streamlined to achieve it, and consider making some of those changes permanent. The default cannot be to revert entirely to the old ways of doing things."**

Among organizations that quickly put in place untethering (typically to support remote work), or that accelerated their large-scale digital transformation, a common comment was, “many organizations are still anchored in old mindsets of compliance and risk avoidance. It is difficult to modernize processes that are decades old and are governed by policies that are also decades old.”

Most interviewees commented that information management needs to be modernized. Information management practices, where they exist at all, are often based around an “in office” business model, with records management performed by moving critical records into a records management system. During the pandemic, most information of importance has been flowing through cloud-based collaboration and communications systems. Although “policy” says such information should still be moved into legacy records management system, few managers interviewed for this paper believe this is happening, and many asked whether it is still a reasonable expectation, or if some new approach is needed.

CONCLUSIONS

Since the publication of *The Risk of the Digital Status Quo* in 2019, there has been an unprecedented shift toward seizing the opportunities that digital tools and processes offer. Digital transformation better prepares organizations for unforeseen change, while legacy technology is associated with an increasing burden of "technology debt" and cybersecurity risk.

Organizations with a desire to be more agile in terms of reacting to crises and building more resilient systems and services should recognize that "digital transformation" is a spectrum, ranging from simple to complex and moving to the cloud does not automatically equate to being digitally transformed. The digital transformation of business processes —that allows an organization to change not only *how*, but *what* work it does —is a lengthy process. The pandemic has shown that ensuring a workforce is "mobility capable" with equipment and infrastructure to "untether" allows an organization to change how they work.

When approaching digital transformation in the development of services, organizations need to consider the integration of smaller, relatively independent components —whether built "in-house" or by 3rd-parties —and accessed on the cloud. While such an architecture maximizes an organization's ability to respond to crises, it takes time to establish and needs to be done in advance. Organizations should also ensure that funding "silos" are not an incentive to maintain obsolete technology practices.

With the greater acceptance of an untethered workforce, there are a range of considerations organizations need to address. The COVID-19 pandemic has emphasized a need for organizations to consider culture and communication, previously provided through informal office interaction, in a remote work environment. For some employees, there is the requirement to offer skills training, including virtual meeting effectiveness, digital literacy and video production skills. For others, predominantly IT staff, the past number of months offered the exciting opportunity to use their skills and training to respond in novel ways to the crisis. Organizations should consider how best to pivot back to an IT environment that keeps employees engaged, promotes the use of their skills and considers the processes change made in response to the pandemic.

Moving to a different post-pandemic environment, especially as organizations consider a hybrid-model of remote and in-office work, there should be a greater emphasis placed on security and privacy requirements. Employee training will help to address some of the security concerns and problems highlighted by the pandemic. Similarly, organizations will need to develop modern, relevant, standard configurations and practices for working remotely, including computing and physical infrastructure. Associated with this is a need to review the streamlined or temporary measures used to implement emergency services and ensure appropriate risk-management decisions are approved and recorded.

Public sector IT leaders have been both responsive and adaptive in navigating the challenges that arose during the pandemic crisis. The experience of Canadian public sector organizations during the pandemic has demonstrated that organizations can move quickly to achieve some degree of digital transformation and to view risk differently. For these organizations, the challenge will be in taking the digital transformation lessons, learned as they reacted to the pandemic, and applying them as Canada moves into a “post-pandemic” world.

APPENDIX: METHODS

ROUNDTABLE

The Roundtable took place on Wednesday, April 20, 2021. Participants included senior public servants from all three levels of government, academics and private sector representatives.

PARTICIPANT LIST

Jeff Bloor
Director General
Digital Enterprise Services Directorate
Information Technology Branch
Canada Revenue Agency

Julian Botham
Student – Contributor
Valencia

Marc Brouillard
Chief Technology Officer/Acting CIO
Treasury Board of Canada Secretariat

Dr. Amanda Clarke
Associate Professor
Carleton University

Katerina Daniel
Director
Transformation and Engagement
Shared Services Canada

Dr. Laura Dawson
Principal Program Manager
Amazon Web Services

Neil Desai
VP / Board Member
Magnet Forensics / Public Policy Forum

Katherine Feenan
Policy Lead
Public Policy Forum

Nicole Foster
Director of AWS Global AI/ML and Canada Public Policy
Amazon Web Services

Alex Holmes
Digital Transformation Leader
Amazon Web Services

Ken Hughes
Director
Ken Hughes Consulting

Masha Kennedy
Director of Partnerships
Public Policy Forum

Richard McDonald
Author
Valencia IIP Advisors Limited

Mike Milito
Assistant Comptroller General, Internal Audit
Treasury Board Secretariat

Michael Power
Managing Director
Privacy
Valencia

Marty Robinson
CIO
City of Medicine Hat

Eric Santor
Advisor to the Governor
Bank of Canada

Shawn Slack
Director
Information Technology and CIO
City of Mississauga

John Weigelt
Chief Technology Officer
Microsoft Canada

INTERVIEWS

Interviews took place between February and March 2021. To protect confidentiality, interviewees are not named; however, those who participated represent the following organizations:

- The Bank of Canada
- Treasury Board Secretariat
- The Government of British Columbia
- The Government of Nova Scotia
- The City of Mississauga
- Legal Aid Ontario
- The City of Medicine Hat
- Amazon Web Services
- Microsoft

ENDNOTE

[1] Donnelly, C. (2020). The coronavirus effect: How Covid-19 is accelerating enterprise cloud adoption. Computer Weekly. https://www.computerweekly.com/blog/Ahead-in-the-Clouds/The-coronavirus-effect-How-Covid-19-is-accelerating-enterprise-cloud-adoption

[2] Baker McKenzie. (2020). 2020 Digital Transformation & Cloud Survey: The Future of Enterprise Data. https://www.bakermckenzie.com/en/insight/publications/2020/10/digital-transformation-cloud-survey-2020

[3] The authors adopted the term *untethered* for use in this paper, because they felt it was a good descriptor for organizations who, prior to the pandemic, had already moved employees to wireless and mobile devices (laptops, Wi-Fi, cellular) even though these employees continued to sit at the same desk. Prior to the pandemic, this mobility facilitated workers' ability to use their tools in alternative meeting rooms or when on business trips, or even to work occasionally from home. When the pandemic resulted in "stay at home" directives, those who were already untethered could easily work from home. Deloitte has also been using the term *untethered* in a similar sense. See: Brinker, M. and Schwartz, J. (2018). The Untethered Workforce: Empowering to 100 percent Mobile Worker. Deloitte Insights. https://www2.deloitte.com/us/en/insights/focus/technology-and-the-future-of-work/untethered-workforce-mobile-workers.html

[4] This, of course, applies to employees whose jobs are not inherently associated with a physical location. Many workers do not have this option, not because of technology but because of the nature of the job.

[5] This assumes that one has access to quality broadband, which enables employees to continue to work at home as they did in the office. For more on this topic, see: Middleton, C. (2021). *Digital Infrastructure for the Post-Pandemic World*. Public Policy Forum. https://ppforum.ca/publications/digital-infrastructure-for-the-post-pandemic-world/

[6] Linthicum, D. (2020). Cloud adoption in a post-COVID world. InfoWorld. https://www.infoworld.com/article/3586597/cloud-adoption-in-a-post-covid-world.html

[7] TechnoMetrica. (2020). 2020 SBEC/TechnoMetrica Small Business Cloud Services Survey. https://sbecouncil.org/wp-content/uploads/2020/06/2020SBECSmallBusinessCloudServicesSurvey-Report.pdf

[8] Microsoft. (2020). New data from Microsoft shows how the pandemic is accelerating the digital transformation of cyber-security. https://news.microsoft.com/en-cee/2020/08/31/new-data-from-microsoft-shows-how-the-pandemic-is-accelerating-the-digital-transformation-of-cyber-security/

[9] Nadella, S. speech cited in Spataro, J. (2020). 2 years of digital transformation in 2 months. https://www.microsoft.com/en-us/microsoft-365/blog/2020/04/30/2-years-digital-transformation-2-months/

[10] McKinsey & Company. (2020). A pandemic digital silver lining: Companies digitized many activities 20 to 25 times faster during COVID-19. https://www.mckinsey.com/featured-insights/coronavirus-leading-through-the-crisis/charting-the-path-to-the-next-normal/a-pandemic-digital-silver-lining-companies-digitized-many-activities-20-to-25-times-faster-during-covid-19

[11] McKinsey & Company. (2020). 2020 year in review: Highlights from our publishing. https://www.mckinsey.com/featured-insights/2020-year-in-review

[12] In the round table discussions, some participants argued that risk appetite had not risen, but rather that risk decisions were being made objectively with better data, e.g., on the risks of alternatives. This argument is consistent with the thesis of the 2019 PPF paper.

[13] Alashhab, Z, et al. (2020). Impact of coronavirus pandemic crisis on technologies and cloud computing applications. Journal of Electronic Science and Technology. https://www.sciencedirect.com/science/article/pii/S1674862X20300665

[14] Microsoft. (2021). 2021 Work Trend Index: Annual Report. https://ms-worklab.azureedge.net/files/reports/hybridWork/pdf/2021_Microsoft_WTI_Report_March.pdf

[15] Carr, B. and Pujazon, D. (2020). Cloud Computing: A Vital Enabler in Times of Disruption. Institute of International Finance. https://www.iif.com/Publications/ID/3978/Cloud-Computing-A-Vital-Enabler-in-Times-of-Disruption

[16] AWS Institute. (2020). How Governments Can Build Resilience in a New Normal. https://d1.awsstatic.com/WWPS/pdf/AWS_How_Governments_Can_Build_Resilience_Whitepaper.pdf

[17] Stone, A. (2020). 2020 Puts Cloud Computing in Government to the Test. Government Technology Magazine. https://www.govtech.com/computing/2020-puts-cloud-computing-in-government-to-the-test.html

[18] Agile is a development methodology that focuses on releasing new capability as a rapidly-paced series of small, incremental deliverables

[19] McKinsey Digital. (2020). Debunking seven common myths about cloud. https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/debunking-seven-common-myths-about-cloud

[20] Amazon. (2020). Cloud Helps Canadian Customers During Covid-19 Pandemic. Amazon Press Release. https://press.aboutamazon.com/cloud-helps-canadian-customers-during-covid-19-pandemic

[21] Deloitte. (2020). A catalyst for cloud: the flexibility to weather the COVID-19-related downturn. https://www2.deloitte.com/lu/en/pages/risk/articles/catalyst-cloud-flexibility-weather-covid-19-related-downturn.html

[22] Kabilan, S. (2019). The Risk of the Digital Status Quo: How Governments Can Enable Digital Transformation. Public Policy Forum. https://ppforum.ca/publications/digital-status-quo/

[23] Office of the Auditor General of Canada. (2021). COVID-19 PANDEMIC; Report 6 – Canada Emergency Response Benefit. at: https://www.oag-bvg.gc.ca/internet/English/mr_20210325_e_43791.html

[24] Gartner. (2020). Predicts 2021: Walking the Walk to an Uncertain Future. https://www.gartner.com/en/doc/predicts-2021-walking-the-walk-to-an-uncertain

[25] McKinsey & Company. (2020). The disaster you could have stopped: Preparing for extraordinary risks. https://www.mckinsey.com/business-functions/risk/our-insights/the-disaster-you-could-have-stopped-preparing-for-extraordinary-risks

[26] Kerrissey, M., and Edmondson, A. (2020). What Good Leadership Looks Like During This Pandemic. Harvard Business Review. https://hbr.org/2020/04/what-good-leadership-looks-like-during-this-pandemic

[27] Bohmer, R., Ives Erickson, J. et al. (2020). 10 Leadership Lessons from Covid Field Hospitals. Harvard Business Review. https://hbr.org/2020/11/10-leadership-lessons-from-covid-field-hospitals

[28] Parent, M. (2021). 5 ways the COVID-19 pandemic has forever changed cybersecurity. Canadian Security. https://www.canadiansecuritymag.com/5-ways-the-covid-19-pandemic-has-forever-changed-cybersecurity/

[29] Smith, A. (2020). In 2020, coronavirus concerns are a cloud security catalyst. Security Magazine. https://www.securitymagazine.com/articles/94086-in-2020-coronavirus-concerns-are-a-cloud-security-catalyst

[30] See, Perlroth, N. and Satariano, A. (2020). Irish Hospitals Are Latest to Be Hit by Ransomeware Attacks. New York Times. https://www.nytimes.com/2021/05/20/technology/ransomware-attack-ireland-hospitals.html

[31] Palmer, D. (2021). Ransomware attacks now to blame for half of healthcare data breaches. ZDNet. https://www.zdnet.com/article/ransomware-attacks-now-to-blame-for-half-of-healthcare-data-breaches/


PUBLIC
POLICY
FORUM