## IBM Center for The Business of Government

## **Emerging Technology for Response and Recovery:** An International Dialogue

Kevin C. Desouza Queensland University of Technology



Given the global nature of the pandemic, collaboration between agencies and across nations proved pivotal to sharing information, innovations, and lessons learned. Information sharing across nations to monitor developments and coordinate responses around the movement of people and goods will become more important as borders open.

–Kevin <u>C. Desouza</u>

## TABLE OF CONTENT

Foreword	4
essons Learned Since the Pandemic	7
Emerging Technologies	
Opening Borders	
Challenges Ahead	13
The Way Forward	15
About the Author	17
Contact Information	
Reports from the IBM Center for The Business of Government	19



## Foreword

In a post-pandemic world, homeland security and border control agencies are being tasked with transforming how they respond and operate in a highly digitalized environment, while ensuring safety and prosperity of citizens and country.

Critical challenges that agencies face include the increasing volume of incidents and emergencies, overly complex trade and immigration processes, and evolving threats to borders and customs. Governments can leverage data, AI, intelligent automation, and other emerging technologies to address these complex challenges—while also freeing up critical human resources for high value missions.

To address these key issues, the IBM Center for The Business of Government hosted an international dialogue in September 2021 attended by CIOs and IT leaders with the Australia Department of Home Affairs, the Singapore Ministry of Home Affairs, and U.S. Department of Homeland Security Customs and Border Protection. These three dynamic leaders engaged in an interactive dialogue, joined by nearly 50 attendees from across the globe.

Professor Kevin DeSouza of the Queensland University of Technology and the Brookings Institution has drawn on this discussion to produce a report providing keen insights about leveraging technologies to improve operations and security across borders. Participants addressed supply chain assurance, opening borders amidst the global fight against COVID-19, and the role of







data, AI, and other technologies to support border security. The wideranging discussion also touched on addressing the needs of the future, anticipating new threats, and developing response strategies. These strategies—which rest on hybrid, multi-cloud environments—include operational capabilities that can stand up "on demand" to address rapidly shifting threats.

This report builds on the Center's body of work that addresses how governments can best leverage emerging technologies to drive effective outcomes. Most recently, this includes Professor DeSouza's report, *Artificial Intelligence in the Public Sector: A Maturity Model*, as well as Gwanhoo Lee's *Creating Public Value Using the AI-Driven Internet of Things*, and Alan Shark's *Innovation and Emerging Technologies in Government: Keys to Success*.

We hope that Professor Desouza's report enables government leaders to draw on insights and lessons learned from across the world.

Daniel J. Chenok Executive Director IBM Center for The Business of Government chenokd@us.ibm.com Don Fenhagen Managing Client Partner IBM Consulting fenhagen@us.ibm.com As governments make their way through the COVID-19 pandemic to emerge stronger, nations are grappling with how to adjust to and plan for the new normal. This future state will fundamentally differ from business as usual before the onset of COVID-19 pandemic.

The pandemic has demonstrated that recovery will last a long while. Nations with good success in limiting casualties from the virus (e.g., Australia) have still not yet fully opened their borders. As of now, Australian citizens and permanent residents can travel internationally but still face quarantine and travel restrictions around interstate mobility.

Singapore has gone through multiple episodes of borders opening and closing. Other countries have also ebbed and flowed between allowing travel to and from 'safe' zones. To make matters more complex, safe zones can vary within a country. For example, as of November 3, 2021, residents of the South Island of New Zealand can travel in Queensland, Australia, while those from the North Island cannot. The movement of cargo between nations is also a complex endeavor that has become more challenging since COVID-19, as global supply chains have suffered severe negative impacts.<sup>1</sup>

Agencies tasked with border control and law enforcement will play a critical role in the response and recovery phase. The IBM Center for The Business of Government recently hosted an international forum with border security and public safety. The goal was to help IT leaders from Australia, Singapore, and the United States to facilitate dialogue on the role that emerging technology can play in ongoing response and recovery efforts. This white paper summarizes salient points discussed during the forum.

1 https://hbr.org/2020/09/global-supply-chains-in-a-post-pandemic-world.

## Lessons Learned Since the Pandemic

Nearly two years since the onset of the pandemic, agencies have learned much about how to respond to mega-scale crises. Agencies tasked with securing borders and customs controls had to intensify operations during the pandemic, and recognized that effective information systems can enable large-scale operations.

#### From Silos to System-of-Systems

The COVID-19 pandemic demonstrated the need to think and operate beyond silos, disciplines, and domains. Tackling crises going forward will require agencies to take a systems approach—more specifically, a systems-of-systems approach as the default mode of operation. Science (research and development) and technology functions will need to work in sync to ensure rapid response. Data and information that reside in systems across agencies will need to be fused together to generate real-time situational awareness. Data from sensors operated by one department will need to feed into analytical engines run by another, which in turn will be integrated with several other information layers to increase the richness of insights. This will need to be assessed by analysts with diverse expertise to arrive at actionable insights.

Government leaders must bring together assets across disparate systems, domains, and organizations. This kind of investment will allow agencies to think and process data collectively, while still preserving the ability to respond in a more decentralized approach where appropriate. Erratic coupling of systems will not suffice to deal with current and emerging threats in the environment. Going forward, the systems-of-systems approach will enable governments to work as an enterprise<sup>2</sup> to solve challenges and take advantage of opportunities more holistically than any single agency can.

The Home Team Science and Technology Agency (HTX) was established in December 2019 to advance science and technology innovation and be a force multiplier to secure Singapore's future. Notably, HTX possesses 15 Centers of Expertise with S&T capabilities that span biometric and profiling, to digital information and forensics, cybersecurity, robotics, automation, and unmanned systems (RAUS), and C41 (Command, Control, Communications, Computers, and Intelligence). HTX brings together interdisciplinary expertise that works across the fundamental science and applied technology spectrum, and ground operations, to anticipate needs and deliver cutting-edge technologies within the Ministry of Home Affairs to solve crimes, save lives, secure borders, and to safeguard Singapore's public spaces.

2 https://www.businessofgovernment.org/report/building-enterprise-government.



#### Collaboration Across the Ecosystem

Among lessons learned from the COVID-19 pandemic is the fact that no single sector or agency has the capacity to respond to a crisis of this scale. Stakeholders across the ecosystem have to collaborate to develop solutions in an agile manner. Within the public sector, focal agencies tasked with responding to crises must have the necessary frameworks and platforms to bring together their various internal units and external partners to solve emergent issues. This is no easy feat to accomplish, given the size and complexity of these agencies and the vast number of entities in the ecosystem. Moreover, protocols must facilitate interagency collaboration to ensure a unified response. Information sharing between agencies must be robust to ensure coordination.

From the production of vaccines to personal protective equipment, the role of public-private partnerships cannot be understated for effective response and recovery. The COVID-19 pandemic has shown how various sectors of the economy can come together and collaborate behind a shared vision (or enemy). However, when recommendations or actions differ across the ecosystem, a lead agency must clarify to avoid bad outcomes.

#### The U.S. Department of Homeland Security's Silicon

**Innovation Program** is a successful collaboration initiative. Its goal is "to find new technologies that strengthen national security with the goal of reshaping how government, entrepreneurs, and industry work together to find cutting-edge solutions. Based in California's Silicon Valley, the program reaches out to innovation communities across the nation and around the world to harness the commercial R&D ecosystem for technologies with government applications and to co-invest in and accelerate technology transition-to-market."<sup>3</sup>

3 https://www.dhs.gov/science-and-technology/svip.

Given the global nature of the pandemic, collaboration between agencies and across nations proved pivotal to sharing information, innovations, and lessons learned. Information sharing across nations to monitor developments and coordinate responses around the movement of people and goods will become more important as borders open.

#### Data-Intensive Computational Systems for Knowledge Discovery

Agencies have had to bolster capabilities around computational systems for real-time knowledge discovery. Emerging technologies such as machine learning, artificial intelligence, and edge computing have played a vital role in helping agencies collect, analyze, and assess an ever-growing swarm of data streams. However, these emerging technologies are only being used for a fraction of the problems that they can solve. The public sector can mature these technologies so that they can be readily deployed, as a recent IBM Center report<sup>4</sup> on an AI Maturity model for government shows.

#### Digitization and Automation of Processes

Where possible, manual processes have been digitized and automated to reduce errors and lags in information processing. Digitizing and automating processes free up personnel from mundane tasks and direct these valuable assets to more cognitive intensive tasks. These technologies can increase speed and accuracy in agency processes.

**The U.S. Department of Homeland Security's Customs and Borders Protection** (CBP) agency employed 50 bots to transfer 30 terabytes of email (about 350 million archived emails) to a new system. This robotic process automation (RPA) saved CBP staff from this mundane task and reduced the migration time for "a terabyte of data from two months to one day."<sup>5</sup> The CBP has 110 bots in operations and is developing another 50.<sup>6</sup>

Australia's Department of Home Affairs will replace its paperbased incoming passenger card with a Digital Passenger Declaration (DPD). The DPD must be completed 72 hours prior to travel to Australia, and will enable verification of COVID-19 vaccination status along with other necessary entry details (e.g., visa status). Relevant data (e.g., health and vaccination status) on international travelers can also be shared with state and territories for contact tracing.

<sup>4</sup> https://www.businessofgovernment.org/report/artificial-intelligence-public-sector-maturity-model.

<sup>5</sup> https://gcn.com/cloud-infrastructure/2019/06/rpa-helps-cbp-migrate-30tb-of-email-inone-day/298051/.

<sup>6</sup> https://www.meritalk.com/articles/cbp-setting-up-ai-innovation-center-cio-bhagowalia-says/.

#### **Real-Time Situational Awareness**

Pressure on agencies to implement real-time situational awareness across multiple environments was significant. Here, agencies faced several challenges. First was the ability to have personnel work seamlessly across classified and unclassified enclaves. Second was the ability to integrate data and systems across heterogenous environments (see previous point on system-of-systems). Third was the requirement to push and pull data from the edges of the organization. Agencies designed and deployed mobile apps to equip frontline agents and operators with necessary information to report critical data.

#### Agile Teams

Deploying teams that can create user-inspired technology solutions with short delivery times ensured that frontline staff had the necessary information to carry out operations effectively and efficiently. Technology teams worked in conjunction with program staff to identify problems and opportunities. Collaboration technologies offer significant promise to bring individuals together who might be geographically and organizationally dispersed to create solutions on-demand and in a plug-n-play manner. This agile approach has worked effectively at multiple levels of government.<sup>7</sup>

#### Security and Reliability of Systems

Maintaining secure and reliable technical systems remains an ongoing challenge. Malicious actors continue to innovate in their attempt to access and compromise mission-critical systems. As governments continue to increase their reliance on information systems and mobile apps to interact and transact with citizens, rogue actors have added incentives to conduct activities such as stealing identities and committing fraud. Failure to stop bad actors can have outsized negative impact on solving border security and related problems.

#### Scaling Systems

Agencies had to look beyond local and small-scale solutions. The pandemic forced agencies to develop capacity to scale systems across domains and environments to address various threats and support response and recovery efforts. This, coupled with improvement in technology, was necessary to successfully resolve problems.

#### **Robust Learning Mechanisms**

In dealing with unchartered waters throughout the pandemic, agencies had to develop robust mechanisms to learn from their operations and scale innovations that showed promise, while pivoting from other efforts. Learning efforts also focused on bringing end-users closer to technology teams and equipping them with necessary knowledge and tools to solve problems on their own.

<sup>7</sup> https://www.businessofgovernment.org/report/adopting-agile-state-and-local-governments and https://www.businessofgovernment.org/report/road-agile-government-drivingchange-achieve-success.

#### **Technological Innovation Roadmaps**

Articulating how technological innovation will shape for the future of agency operations became vital to guide investment decisions. Agencies will benefit from preparing five- to ten-year roadmaps of how they plan to exploit technological affordances to drive mission excellence.



## **Emerging Technologies**

Technologies drove response and recovery efforts.

- **Advances in biometrics** help shape travel across borders from both a security and a user-experience viewpoint.
- **Distributed ledger technologies**, primarily Blockchain, offers significant promise to verify credentials (e.g., vaccination status) across multiple environments and contexts.
- Robotic process automation enables agencies to automate where they needed to increase process efficiencies and free up vital human resources.
- **Cloud computing** solutions play a key role in enabling data sharing and access to applications across the public sector ecosystem.
- **Edge computing** solutions push and pull information from the frontlines.
- Data science and machine learning applications help make sense of vast troves of data, connect the dots in real-time, and discover actionable knowledge.
- Simulation and modeling enable agencies to conduct what-if-scenario analyses, understand the intended and unintended consequences of response strategies, and to more holistically engage necessary stakeholders in planning.

While advances in technologies supported response and recovery efforts, further opportunities exist. For example, CCTV data can aid contract tracers to identify those who might be exposed to a virus. This data, coupled with check-in data from contract tracing apps, can enable rapid response to local outbreaks. However, leveraging data requires agencies to have collaboration protocols in place across the levels of governments. Moreover, data must be used ethically and legally to protect the rights of citizens.



## **Opening Borders**

In a world with increasingly open borders, agencies will need to maintain vigilance across the environment and have the capacity to respond instantaneously and decisively in the face of threats. Below are key initiatives agencies can focus on to ensure that people and goods have a seamless and secure travel experience.

- **Increasing the speed** by which data can be fused together across multiple contexts and environments, to ensure that operators have access to the best intelligence to execute their work
- Linking different systems through permission-driven platforms to give users a unified and system-level view on key issues, activities, and domains
- Enhancing interoperability of systems and creation of standards and frameworks to promote sharing of vital information across agencies, sectors, and nations
- Fusing data, technologies, systems, and domains of expertise together to design command centers of the future that operate at the systems-of-systems level
- **Creating use cases** to drive innovation and solution development that bring together capabilities across entire ecosystems
- **Exploring scenarios** (e.g., pre-vetting of capabilities and capacity) to leverage trusted partnerships with industry in an agile manner
- Investing in designing next-generation cybersecurity capabilities aligned with the dynamics of current and future environments. For instance, more dynamic vetting of credentials for access that is temporal or spatially restricted
- **Designing next-generation technologies** (e.g., mobile apps) to communicate with citizens to increase transparency, accountability, and trust. As borders open there will be a need to involve the public as agencies consider risk management strategies to address future events.

## **Challenges Ahead**

Critical threats and challenges will emerge as governments continue to address the COVID-19 pandemic.

#### Speed to Collaborate

As discussed above, collaboration across ecosystems has ensured effective response and recovery efforts. Going forward, however, agencies will need to proactively setup procurement options and cannot afford to reactively backfill procurement needs during crises. Agencies can work proactively with external partners that are pre-vetted based on capabilities assessed, especially as the pressure to reduce the time to market continues to intensify. Therefore, agencies need protocols to pre-emptively assess capabilities and competencies of partners and vet them as required to adhere to security requirements. As the ecosystem expands in unexpected ways, the need expands for a nimble approach to collaboration.

#### **Open Source**

Today, open platforms have flourished that provide data and applications. Open source intelligence provides a viable source of critical insights on key threats facing societies. While the benefit of leveraging open-source applications remains strong, many perceive this to be tempered by increased risk from security threats. Much work remains to institute policies and frameworks that enable agencies to take full advantage of open source applications. This is especially true for valued computational systems that constitute the backbone of a nation's critical digital infrastructure. The promise of open source is simply too great to push aside.

#### Cybersecurity

While agencies have invested significant resources to secure digital assets and systems, the threats they face continue to evolve. Advanced Persistent Threats (APTs) from non-state actors, in some cases heavily resourced by state actors, are increasing in sophistica-



tion. Cyber-physical critical infrastructure has interested these rogue actors to cause widespread havoc both in the digital and physical arenas. In addition, criminals continue to exploit weaknesses in systems and nondigital processes to compromise systems and disrupt the delivery of public services. Ransomware incidents on the rise for the last few years have targeted local governments.

#### **Evaluating Vitality of Response Capabilities**

A nation's response capacity and capability depend on its stockpile of critical assets. As COVID-19 has shown, even the most advanced nations faced a shortage of ready-to-use critical equipment (e.g., personal protective equipment—PPE—for healthcare professionals). While nations have amassed stockpiles to prepare for various crises, such assets should be examined to ensure that they remain fit-for-purpose. Response capabilities are not solely relegated to the public sector; the private sector plays a critical role in enabling a swift response to a crisis, whether in the production of PPEs or in the creation of a vaccine. Hence, the public sector must engage with the private sector to understand what capacity exists, and the most effective ways to access such capacity in a crisis.

#### **Combating Misinformation**

The rise of misinformation severely threatens a nation's stability. The sources of misinformation are as diverse as the scope misinformation generated and then propagated over various networks. The very technologies that keep citizens informed about threats and response efforts, such as social media, are the biggest culprits in spreading misinformation. The inability to combat misinformation leads to several negative outcomes, such as limiting the effectiveness of response strategies (e.g., those that do not follow lockdown restrictions or anti-vaxxers), creating alternative threats that need law enforcement resources, and eroding the trust in the public sector. As the use of this ecosystem grows, the need for message accuracy from governments also needs to grow. A well-meaning member of the ecosystem could inadvertently say or do the wrong thing, and fixing the problem and regaining trust will be a challenge.

#### Citizen Engagement

Crises like the pandemic require the public to be active solution contributors and add constraints. COVID-19 brought a new set of restrictions that impacted all facets of life, from travel domestically and internationally to extended lockdowns to contain the virus spread. While most people have complied with regulations, the patience of the citizenry has been tested. The public sector will need to reengage with citizens about requirements to prepare for the next crisis. While the first point of citizen contact are local governments, a coordinated strategy will connect up with state and federal agencies.

The engagement and preparation of citizens can make a huge difference in responding to already complex crises. Consider events such as the Boston Marathon bombings, where citizens readily shared images and videos to help law enforcement agencies apprehend the terrorists. To this end, increased trust between citizens and government is vital. Communication protocols can increase transparency, accountability, and engagement to drive the co-creation of solutions with citizens.



## The Way Forward

As governments move forward during the COVID-19 pandemic and as borders ultimately reopen, nations will enter unchartered territory. The pressure on governments to be vigilant, and take decisive actions as environmental conditions warrants, will be unrelenting. Agencies tasked with securing borders and law enforcement have made great strides to prepare for the new normal. Yet much work remains. In particular, the public sector should:

- Bring together stakeholders across sectors from private enterprises to nonprofits, nongovernmental organizations, and academia to work collaboratively to tackle grand challenges (e.g., securing critical infrastructure), and bolster capacity to respond to crises. The holistic focus of this should address people, process, and technology issues.
- Develop the capacity for anticipatory governance to get ahead of crises. This will require a relentless focus on increasing situational awareness across heterogenous environments. Insights discovered must be actioned in a decisive manner to prevent threats from gathering speed and materializing into large-scale crises that can explode internationally.
- Leverage technological advances to optimize current operations and service delivery, and to reimagine how agencies might achieve mission objectives. Emerging technologies can open up new opportunities for organizational effectiveness. Designing around mission objectives and future operating environments will enable agencies to move away from legacy administrative processes, protocols, and systems.

• **Constantly evaluate how emerging technologies** are used in an ethical manner that adheres to laws and regulations. The public must trust agencies to do the right thing, especially when trust in public agencies and elected officials continues to remain low. Agencies must continue to evaluate how they balance privacy and rights of sovereign citizens, while addressing risks from crises.

While COVID-19 has dominated minds since its onset in early 2020, governments must remember that this is just one risk factor—others include political and social unrest, declining trust in government, climate emergencies, and fragile states. The public sector has been resilient in the face of these multiple crises, as demonstrated by actions taken in border security agencies from Australia, Singapore, and the United States.

The ingenuity and dedication to keeping nations safe and secure must be valued and treasured. Government leaders need the best possible tools and knowledge to tackle increasingly complex environments. Emerging, advanced technologies can allow the public sector to secure mission objectives.



## About the Author



**Kevin C. Desouza** is a professor of Business, Technology and Strategy at Queensland University of Technology (QUT). At QUT, he leads the Robust Enterprise theme within the Centre for Future Enterprise and is co-leader of the Government Systems Domain in the Centre for Data Science. He is a nonresident senior fellow in the Governance Studies Program at the Brookings Institution. He formerly held tenured faculty posts at Arizona State University, Virginia Tech, and

the University of Washington. He holds or and has held visiting appointments at the London School of Economics and Political Science, Università Bocconi, Shanghai Jiao Tong University, the University of the Witwatersrand, and the University of Ljubljana.

Desouza has authored, co-authored, and/or edited nine books. He has published more than 150 articles in journals across a range of disciplines including information systems, information science, public administration, political science, technology management, and urban affairs. Desouza is the author of four reports for the IBM Center for The Business of Government, *Delivering Artificial Intelligence in Government: Challenges and Opportunities, Creating a Balanced Portfolio of Information Technology Metrics, Challenge.gov: Using Competitions and Awards to Spur Innovation and Realizing the Promise of Big Data.* 

Several outlets have featured his work including *Sloan Management Review, Stanford Social Innovation Research, Harvard Business Review, Forbes, Businessweek, Wired, Governing, Slate.com, Wall Street Journal, USA Today, NPR, PBS, and Computerworld*. Desouza has advised, briefed, and/or consulted for major international corporations, nongovernmental organizations, and public agencies on strategic management issues ranging from management of information systems to knowledge management, innovation programs, crisis management, and leadership development. Desouza has received over \$2 million in research funding from both private and government organizations.

For more information, please visit: http://www.kevindesouza.net.



## **Contact Information**

Kevin C. Desouza Professor of Business, Technology and Strategy QUT Business School Faculty of Business & Law Queensland University of Technology

Email: kevin.c.desouza@gmail.com Twitter: @KevDesouza Web: http://www.keivndesouza.net

# REPORTS FROM THE IBM CENTER FOR THE BUSINESS OF GOVERNMENT

For a full listing of our publications, visit www.businessofgovernment.org

#### Recent reports available on the website include:

## Agility:

Adopting Agile in State and Local Governments by Sukumar Ganapati The Road to Agile GOVERNMENT: Driving Change to Achieve Success by G. Edward DeSeve

### Digital:

Artificial Intelligence in the Public Sector: A Maturity Model by Kevin C. Desouza Aligning Open Data, Open Source, and Hybrid Cloud Adoption in Government by Matt Rumsey, Joel Gurin

### Effectiveness:

Managing The Next Crisis: Twelve Principles For Dealing With Viral Uncertainty by Katherine Barrett and Richard Greene, Donald F. Kettl

*Other Transactions Authorities: After 60 Years, Hitting Their Stride or Hitting The Wall?* by Stan Soloway, Jason Knudson, Vincent Wroble

## Insight:

Delivering on the Vision of Multi-Domain Command and Control by Dr. David Bray Using Technology and Analytics to Enhance Stakeholder Engagement in Environmental Decision-Making by Jenna Yeager

## People:

The Age of Remote Work: How COVID-19 Transformed Organizations in Real Time by David C. Wyld

Reskilling the Workforce with Technology-Oriented Training by Stacie Petter, Laurie Giddens Sustaining a Distant Vision: NASA, Mars, and Relay Leadership by JW. Henry Lambright

## Risk:

*The Rise of the Sustainable Enterprise* by Wayne S. Balta, Jacob Dencik, Daniel C. Esty, Scott Fulton

Managing Cybersecurity Risk in Government by Anupam Kumar, James Haddow, Rajni Goel



#### About the IBM Center for The Business of Government

Through research stipends and events, the IBM Center for The Business of Government stimulates research and facilitates discussion of new approaches to improving the effectiveness of government at the federal, state, local, and international levels.

#### About IBM Consulting

With consultants and professional staff in more than 160 countries globally, IBM Consulting is the world's largest consulting services organization. IBM Consulting provides clients with business process and industry expertise, a deep understanding of technology solutions that address specific industry issues, and the ability to design, build, and run those solutions in a way that delivers bottom-line value. To learn more visit ibm.com.

For more information: Daniel J. Chenok Executive Director IBM Center for The Business of Government

600 14th Street NW Second Floor Washington, D.C. 20005 202-551-9342

website: www.businessofgovernment.org e-mail: businessofgovernment@us.ibm.com



#### Stay connected with the IBM Center on:



or, send us your name and e-mail to receive our newsletters.