Microsoft

Advancing cyber resilience with cloud computing

Authors

Paul Nicholas
Kaja Ciglic

Contributors

Theo Moore
Bruce Johnson
Jim Pinter
Tyson Storch
Jessica Zucker

Introduction

Economies, societies, and governments around the world are being challenged and reinvented by emerging technologies such as social media, big data and the Internet of Things (IoT). As governments' operations become more data-driven and ICT-centric, they need to be made as resilient as possible not only to cyber-threats but also to the wider range of natural and man-made disasters that can occur. At the same time, the role of these new technologies in wider crisis planning, preparation and response needs to be addressed.

Incorporating cloud into digital continuity plans has substantial benefits.

With this white paper, Microsoft seeks to address how hyperscale cloud computing infrastructure ("the cloud"), can enhance digital continuity and cyber resilience for governments and the public sector more broadly. It looks at the role commercial cloud can play in giving a government, at the national, regional or city level, the capacity to maintain its services and the data it needs to function, regardless of adverse developments and crises.

Governments' options for ensuring cyber resilience and digital continuity have been greatly expanded by the emergence of the cloud thanks to its geographic distribution, scalability, security and cost-effectiveness. Incorporating cloud into digital continuity plans has, therefore, substantial benefits.

Before a government can realize this potential, however, there are likely to be technical and policy challenges that will need to be addressed. Technical issues, for example the practicalities of achieving "failover" into the cloud for an important government digital service during a crisis, are less likely to be a significant challenge than policy issues. Therefore one challenge is likely to be the cross-border nature of the cloud's infrastructure, which helps to underpin many of the cloud's strengths in resilience and continuity, but which also raises inevitable questions about the transfer of confidential or private data out of a government's jurisdiction and, notionally at least, out of its control.

The aim of this white paper is, therefore, to help policy-makers and civil servants better understand, in general terms, the processes by which these challenges can be addressed and why the benefits of incorporating commercial cloud into governmental cyber resilience and digital continuity plans make this effort worthwhile.

Contents

Cloud computing in government resilience and continuity

Cyber resilience can best be understood as an organization's capacities and capabilities for readiness, response, and reinvention in the face of a cyber threat. For any tier of government this includes processes that enable stability, ensure recovery and help restore services rapidly. In other words, for governments at the national, regional or city level cyber resilience ensures that services can continue to be available and operate without being compromised, whether by cyber threats or by the impact of natural and man-made disasters.

Digital continuity is one means by which any organization, government or otherwise, can develop its cyber resilience. Its purpose is to maintain digital services and data relevant for the functioning of those services, regardless of any adverse changes or interruptions.

Digital continuity is distinct from another important aspect of cyber resilience: cybersecurity. Cybersecurity is about protecting the confidentiality, integrity, and availability of data, ICT systems, and ICT infrastructure. Digital continuity is about an ICT system's ability to continue delivering as intended, even if cybersecurity is failing or has failed.

The role of cloud computing in digital continuity or cyber resilience is a recent consideration for many states, regions and cities. However, governments are increasingly taking advantage of new technologies and in some countries many government services now exist primarily or only in digital format. These services can often be critical not only to the functioning of the state, region or city but also to citizens' ability to exercise their rights and fulfil their responsibilities. Maintaining those digital services, especially in a crisis, has required new risk management thinking and operational practices for governments. As a consequence, governments of all sizes are now turning to digital continuity, and are looking at the role that cloud can play.

> ...governments of all sizes are now turning to digital continuity, and are looking at the role that cloud can play.

Components of cyber resilience

Readiness. To plan for long-term readiness, an organization must identify assets, assess and manage infrastructure risk, develop capabilities to respond to and recover from disruptions, and invest in research, education, and practices that contribute to long-term cyber-resilience goals.

Response. Using the plans and strategies set in place during the readiness phase, resilient entities continue to function during a crisis and rebound quickly. A resilient response is also adaptive and flexible: innovating during a crisis is a key element of resilience.

Reinvention. Learning from and improving on existing plans and strategies is a hallmark of cyber resilience. After a crisis has passed, analysis is key: identifying what was effective and where the response was problematic; developing a plan for improvement; and then implementing that plan. It's important to think beyond short-term gains.

The practical benefits of cloud computing for resilience and continuity

As their operations become more data-driven and ICT-centric, governments and public sector organizations must ensure that their services and data are as resilient as possible, and that they can be restored quickly in times of crisis. Cloud can help this, supporting existing approaches to resilience and continuity whilst also providing new options due to its distribution, scalability, security and cost-effectiveness.

Geographical distribution

A key feature of cloud is the geographic failover capability that could protect critical services from the consequences of a major crisis, e.g. a natural disaster, a critical infrastructure failure or a significant attack. However not all states, regions or cities are exposed to the same threats. If such threats are part of a government's wider risk assessments, then the case for cloud in support of both digital continuity as well as overall resilience is particularly strong.

A key feature of cloud is the geographic failover capability that could protect critical services from the consequences of a major crisis.

Most specific risks, e.g. earthquakes or flooding, tend to be concentrated in particular locations or geographies. Major cloud vendors, however, typically run multiple datacenters across several different sites, states and continents, and replicate customer data in two or more locations. This allows them to provide robust service levels and data resilience in the face of geographically focused risks. Moreover, with centralized data storage, management, and backups, data recovery in response to local disruptions can be faster and easier. If an organization loses access to its on-premises servers in a crisis, cloud providers can continue to safeguard data and support essential government services. In fact, many cloud vendors back their assurances of data availability by offering a service level agreement that provides 99.99 percent uptime to their customers. As one expert has noted, protecting against data loss "is the objective of [having] geographically separated, secure, duplicate, redundant computing services. Commercial cloud service providers know very well what has to be done to maintain continuity of operations under just about any known conditions..."[1]

Cloud resilience in Hong Kong

"Resilience is a big step forward for business continuity. It is much more than data back-up and recovery, as true resilience requires dynamic and seamless initiatives to provide highly-secure assurance to business."
- Hideaki Ozaki, President and CEO of NTT Com Asia

Since 2016 Microsoft has offered a cloud solution dedicated to cyber resilience in Hong Kong. The solution is a partnership with NTT Communications and leverages their Enterprise Cloud services and ICT infrastructure and Microsoft's Azure cloud and ExpressRoute private tunnel, which ensures that customer data does not travel over the public internet. It is estimated that the cost of the offer is about 55% that of a self-built, back-up solution.

[1] Paul Wormeli, IJIS Institute, Mitigating Risks in the Application of Cloud Computing in Law Enforcement 22 (2012), available at http://www.businessofgovernment.org/report/mitigating-risks-application-cloud-computing-law-enforcement.

Scalability

Cloud services can provide colossal levels of computing power effectively on demand, meaning that government departments and agencies can use these services as fail-over for their own systems as and when needed. Taking full advantage of this would, however, require the relevant government system to maintain active contracts with cloud service providers and to keep a skeleton-version of the infrastructure running in the cloud. This would have funding implications.

Because certain government data and services are likely to be in particularly high demand during times of crisis, the highly scalable and "elastic" nature of cloud computing means systems supporting these services are less likely to crash, even under unusually heavy usage requirements. The Organization of Economic Cooperation and Development (OECD) has noted that the "elasticity" of cloud computing is one of its great strengths: "*Computing resources can be provisioned in an elastic and rapid way that allows adaptation to changing requirements such as the amount of data supported by a service or the number of parallel users.*" [2]

The majority of innovation is delivered in the cloud and only later translated into on-premises solutions.

Security

Cloud providers recognize that trust is a fundamental part of their business model and do their upmost to keep it. At the same time, they operate on a scale that requires them to design and build their systems based on the assumption that anything that can go wrong will go wrong, e.g. nefarious users will exist, customer workloads will sometimes be infected with malware, or physical machines, network devices, and storage arrays will fail. Providers therefore need to maintain complete control of the environment and enforce best practices and secure defaults for tenants.

The large pool of clients can also work to the benefit of security, as it allows cloud providers to look for security intelligence across their whole environment, which is much larger than an average corporation's traditional on-premises infrastructure. This data can be used by big data security-intelligence systems to discover malware and network intrusion attempts around the globe. The faster such threats are identified, the better chance there is of stopping malware before it infects a cloud provider's client.

Finally, it is important to acknowledge that most technology providers have adopted a "cloud first" approach. As a result, the majority of innovation is delivered in the cloud and only later translated into on-premises solutions. Given the comparative speed of updates in the two environments, this represents a significant advantage for cloud over traditional implementations, especially as many of these developments are in security.

[2] OECD, Cloud Computing: The Concept, Impacts, and the Role of Government Policy (2014), available at http://www.oecd-ilibrary.org/science-and-technology/cloud-computing-the-concept-impacts-and-the-role-of-government-policy_5jxzf4lcc7f5-en.

Cost-effectiveness

Most commercial cloud services are available on an as-used, pay-as-you-go or subscription basis. This means data can be stored and secured using the latest software and hardware; something that would have cost thousands of dollars in the past is now provided at a fraction of the cost. Furthermore, because resources are elastically provisioned, they can quickly scale, and organizations will pay for computing resources only when they need them. This can be particularly helpful for government functions such as processing tax returns or deploying snow removal equipment that experience predictable spikes in usage and capacity.

> ...something that would have cost thousands of dollars in the past is now provided at a fraction of the cost.

Nevertheless, an analysis of potential extra costs needs to be conducted to understand the full scope of the work. Such costs include the necessary rebuilding of the architecture for those services, the maintenance of duplicate services (on premises and in the cloud), and training staff to manage a more complicated architecture. In sum, governments could in theory use commercial cloud to avoid having to invest substantial resources not only in purchasing, but also in building and maintaining their own systems, only to see them sit idle most of the time. For this reason "using the cloud as a [disaster recovery] platform makes it more affordable to create a truly durable implementation by replicating systems and data across multiple geographies." [3]

Policy foundations needed for use of cloud for resilience and continuity

While there appears to be a practical case for the use of cloud services in digital continuity and disaster recovery plans, relatively few governments have formal policies that encourage its use. In fact, many have policies in place that could make it difficult for government departments and agencies to take advantage of the cloud's geographical distribution, scalability and cost-effectiveness.

At the same time, approaches to the use of cloud in digital continuity and cyber resilience plans that suit one state may not suit another. This may be due to differing geopolitical realities, national infrastructures or modus operandi. Differing physical geographical locations may also bring specific environmental factors that affect the relevance or feasibility of using cloud technology, whilst differing levels of technical capability may also make some options less practical.

Policy and legal challenges may also arise. The scope for reliance on cloud in continuity and resilience plans for any country, region or city will depend on their legal structures, their risk management approach and their assessment of the threat landscape. Overall, the national legal framework is likely to determine much of the context for regional or city tiers of government. The issues to be addressed could include public sector procurement and expenditure rules, security standards and frameworks, and auditing.

[3] Lauren Whitehouse and Jason Buffington, Enterprise Strategy Group, Amazon Web Services: Enabling Cost-Efficient Disaster Recovery Leveraging Cloud Infrastructure 3 (Jan. 2012), available at http://d36cz9buwru1tt.cloudfront.net/ESG_WP_AWS_DR_Jan_2012.pdf

Of particular importance will be policies that govern the handling of data held within government systems, specifically the transfer of data across national borders. One of the fundamental ways in which cloud achieves its resilience is through geographical distribution over multiple data centers in different jurisdictions. A crisis hitting one is unlikely to affect the others, outside of a global catastrophe. However, any tier of government preparing to use the cloud will have to consider what that cross-jurisdiction transfer will mean for its data or the data of its citizens. Can data that resides in a particular state be transferred outside of its territory? If so, where to? Which statutory authority or agreed procedure determines when this happens and how? How can the state ensure that data is being handled in a responsible and secure manner outside of its jurisdiction? Is data outside a state's jurisdiction if it resides in the cloud or in a virtual "data embassy"?[4] In extreme situations, can critical state functions be moved to the cloud, even outside a country's physical territory, and how can these functions be secured in a way that meets public expectations, not least of all security and privacy?

It is essential that such policy complexities be addressed as seriously as challenges that are technical or infrastructural.

When building digital continuity capacity it is essential that such policy complexities be addressed as seriously as challenges that are technical, infrastructural, etc. Based on a review of several jurisdictions,[5] including some that have embraced the move to digital data and services in government, several policy-related areas need to be addressed as part of enabling the use of cloud services for government digital continuity and disaster recovery planning. This is the case even when the government fully endorses the use of cloud computing, for example by adopting a "cloud first" policy or strategy, as the Philippines[6] or the United States[7] have done, or by incorporating a "no legacy system" approach, as is the case with Estonia.[8]

[4] Estonia to establish the world's first data embassy in Luxembourg, June 20, 2017, see https://www.eesistumine.ee/en/news/estonia-establish-worlds-first-data-embassy-luxembourg

[5] Including Australia, Estonia, Germany, Japan, Korea, Norway, the United Kingdom, and the United States.

[6] The Philippines Cloud First Policy: http://i.gov.ph/policies/signed/department-circular-cloud-first-policy/ and National Cybersecurity Plan 2022: http://www.dict.gov.ph/national-cybersecurity-plan-2022/

[7] United States Federal Cloud Computing Strategy: https://www.dhs.gov/sites/default/files/publications/digital-strategy/federal-cloud-computing-strategy.pdf

[8] Estonian e-government Strategy: https://www1.oecd.org/governance/observatory-public-sector-innovation/blog/page/e-estoniatakesdigitalgovernmentinnovationtonextlevel.htm

The Philippines: Cloud First Policy

The announcement in January 2017 of a cloud first policy in the Philippines needs to be seen in the context of the government's objective to increase its cybersecurity and resilience, as per the National Cybersecurity Plan 2022.

The government's decision to endorse cloud computing is driven by the desire to cut cost, increase employee productivity and improve citizen online services. At the same time, the government is consciously moving away from legacy systems in an effort to improve the cyber resilience of its operations: "*The cloud first model enhances government ICT resiliency and security as version upgrades to both hardware and software are managed by the cloud service provider*".

The reason for this is that cyber resilience encompasses a much broader set of issues than simple ICT procurement. To enable it, governments should look beyond its security standards and frameworks, although these are not be neglected. For example, it is "information/digital society" laws that tend to establish requirements pertaining to digital service providers, most notably governing issues related to supervision and liability. Similarly, it is "electronic communications" or "cybercrime" laws that often ensure protection of users and set the scope of law enforcement powers in interception, etc. Equally important, "freedom of information" laws more often than not regulate access to information created or held by government. "Data classification" laws define types of restricted information and the grounds for granting access to them. And, "personal data protection and data privacy" laws categorize information types and their appropriate levels of protection, along with relevant oversight and liability.

More often than not, these laws have been written not only for a pre-cloud but pre-internet era.

Finally, laws and policies that deal with procedures and process, as they relate to emergencies, need to be examined. These tend to enable, control, or limit government action during various types of national emergency. They are important as they outline the course of action that needs to be taken, as well as the roles and responsibilities of various stakeholders involved. More often than not, these laws have been written not only for a pre-cloud but pre-internet era.

As governments and other public sector entities are revising their existing frameworks with the intention of embracing a cyber resilience posture, they should particularly look to prioritize the following:

1 Invest in robust broadband infrastructure

A fast and ubiquitous broadband infrastructure is a fundamental prerequisite to the successful use of cloud services, especially in the context of disaster recovery. It is recommended that an assessment of the provision of broadband services is conducted.

2

Modernize procurement rules and requirements

Embracing cloud computing for cyber resilience frequently requires an adjustment in how an organization deals with its financing. Specifically, ICT purchases tend to typically fall under "one off" capital expenditures (cap ex), whilst cloud computing allows for more flexibility in that regard, given that it operates as a pay-per-use model. As a result, rules might have to be adjusted to allow for ICT purchasing under operating expenditure (op ex) for an "ongoing service".

3

Assess data residency requirements

Countries frequently have data residency requirements in place, in particular when it comes to data that is classified as essential. To ensure that cloud computing can be used to its full potential, we recommend that an assessment is made of which data is in effect open data and that restrictions on its storage are then lifted. Moreover, in the context of digital continuity and recovery scenarios, we recommend that exceptions are written even for the most critical of data.

4

Utilize international standards for security assurance

Transparent security assurance continues to be a concern for organizations thinking about moving to the cloud. Security is even more critical for government and public sector organizations looking to utilize cloud computing for digital continuity. However, instead of seeking to develop their own requirements, we recommend organizations utilize internationally aligned security requirements that have been tried and tested by others. These have not only been proved to be effective, but can be deployed immediately, whilst developing requirements from scratch can take years.

5

Allow for a level of flexibility on auditing of cloud vendors

In the context of cloud, governments and public sector organizations need to adjust their existing models of security assessments. As cloud computing represents a shared services model, numerous customers share its infrastructure at any given time. Direct auditing of the service is therefore not only impracticable but could endanger security of the service. To this end we recommend that organizations accept third party certifications from established international auditors as an alternative.

6

Encourage transparency between all parties involved

Increased transparency between governments and cloud vendors is required to build and maintain public trust. This relates to both vendors providing assurances around their security and privacy commitments, as well as to governments detailing their own policies, practices and objectives.

Additionally, whilst not strictly a matter of pure policy, governments of any scale should be cautious when considering the development of their own private cloud solutions. Whilst technically possible, many such efforts have failed to deliver the resilience, continuity and cost benefits that come from using existing commercial cloud. Public sector organizations should consider if it is a good use of this resource to effectively compete with the private sector services that already exist at sufficient scale, that meet legal and regulatory requirements, and that could be bought in as such.

Cyber resilience best practices

Cyberattacks, natural disasters and the like do not cause problems just for IT departments.

Digital continuity is one aspect of the wider cyber resilience agenda. One of the major challenges to building an effective long-term cyber resilience strategy and implementation plan is accurately characterizing and quantifying the core capabilities needed. Drawing heavily on the Threat and Hazard Identification and Risk Assessment Guide published by the US Federal Emergency Management Agency (FEMA),[9] we recommend five key steps to that essential process:

1. **Identify key threats and assess their impact on critical systems and functions.**
2. **Classify and prioritize critical services.**
3. **Set cyber resilience goals and objectives.**
4. **Develop desired cyber resilience outcomes and identify and test capabilities.**
5. **Define roles and responsibilities and determine resources needed.**

Understanding cyberthreats and estimating their likelihood can be problematic. There are many malicious actors, motives and attack vectors. Some attacks may simply be preludes to others. The complex relationships between systems may give rise to unanticipated cascading effects more severe than the damage originally intended by the hacker. Finally, the nature of the damage may not be immediately obvious, for example the exfiltration of data from sensitive systems or even more disconcertingly alteration of critical data.

Prioritizing which critical services and sensitive information to protect involves tough trade-offs. Identifying all services and assets as high priority is not practical, so it is necessary to define and implement a clear framework for classifying data and services (including those operated by third parties) as high, medium, or low impact. The National Institute of Standards and Technology (NIST) offers one such framework: Standards for Security Categorization of Federal Information and Information Systems.[10] Once services are classified, prioritizing them must be grounded in a solid understanding of the inner workings of each service and how it is connected to and dependent on other services. The NIST Framework for Protecting Critical Infrastructure Cybersecurity[11] is an authoritative resource that can help with making risk-based security decisions.

Before goals and objectives can be set, key stakeholders must have a clear and common understanding of their vision for cyber resilience, one that reflects societal values, traditions, and legal principles. This is the foundation for what will be a collaborative effort to set goals that describe a high-level desired outcome or capability, and supporting objectives. It is essential these goals and objectives are flexible enough to accommodate inevitable changes in governmental organization and in technology. Cyberattacks, natural disasters and the like do not cause problems just for IT departments. They can create political and social unrest by physically destroying hardware and data. Therefore, any resilience strategy needs to specify its desired outcomes, and then identify the capabilities necessary to respond to identified threats and successfully deliver those outcomes. As described in the FEMA guide, "*Desired outcomes describe the time frame or level of effort needed to successfully deliver core capabilities. Capabilities are only useful if*

[9] See: https://www.fema.gov/media-library-data/8ca0a9e54dc8b037a55b402b2a269e94/CPG201_htirag_2nd_edition.pdf
[10] See: http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf
[11] See: www.nist.gov/cyberframework

communities can deliver them in a timely and effective manner."[12] When it comes to cyber resilience, success can be defined either as the delivery of capabilities within a certain time frame or in terms of percentages of critical functions restored.

Determining the resources needed for cyber resilience starts with a functional understanding of the critical services developed in the second step above. Considered through the lens of resources required it becomes practical to identify the people and skills, the technology and funds needed. Starting with a matrix of key stakeholders and technology owners, clearly identify who is responsible for each functional area when responding to a crisis, assign and clarify specific responsibilities for those roles, and determine what resources are available to them. Defining roles can be a difficult task at any level of government, from a national down to a particular city. Role assignments may need to cut across traditional lines of authority, with shared accountability and responsibility. Without clarity, however, in a crisis there could be conflict over who is to supposed to do what. Additionally, other resources will need to be put in place, from technical support through to options such as digital continuity to ensure the ongoing functioning of key services.

[12] See: https://www.fema.gov/media-library-data/8ca0a9e54dc8b037a55b402b2a269e94/CPG201_htirag_2nd_edition.pdf

Microsoft's recommendations on resilience and continuity in the cloud

Implementation of cloud computing services requires public sector entities to adapt a forward-leaning technology posture.

Our experience working alongside organizations and governments around the world has shown that cloud computing can be a practicable and valuable tool for cyber resilience and digital continuity. Thanks to its geographic replication of data, rapid scalability, security features and cost-effectiveness, cloud enables users to increase the efficiency of their operations and their agility in response to threats. It also allows for high availability and resilience, and it provides the opportunity for seamless and controlled failover from local, on-premise systems to remote data centers secure from localized natural or man-made threats.

Furthermore, an effective and cyber resilient implementation of cloud computing services requires public sector entities to adapt a forward-leaning technology posture that will ensure a mindset that is continuously on the lookout for security improvements. To do so Microsoft believes governments of all sizes should consider the following actions:

1

Adopt a posture of cyber resilience and digital continuity.

For all organizations, cyber resilience and digital continuity begin with strategic decisions that signals change across a range of areas, from cybersecurity posture to data classification. Although cloud is only one of the technologies that can help governments, its usage requires a comprehensive cross-organizational approach to that specifies the desired resilience and continuity outcomes, identifies critical systems and threats to them, and is executed with roles and resources allocated to specific tasks as required. This is a shift from simply delegating solutions to IT departments and is focused on all workers learning and evolving.

2

Determine which data and services will be migrated to the cloud.

Public sector organizations should each have their own data classification framework in place, and their data and services should already be assessed, classified, and treated in accordance with the risk profiles assigned in those frameworks. However, once the organization makes the decision to utilize cloud computing as part of its cyber-resilience efforts, an additional risk assessment should be conducted. The latter should, among other things, include:

- An examination of whether the organization's current ICT infrastructure would be able to provide the necessary resilience in case of a disruption, and a clear identification of weak spots, as well as opportunities to address them;
- An assessment of the risks associated with replicating in or migrating data and services to the cloud for disaster recovery purposes;
- An understanding of how important the speed of access to a particular set of data or services would be in the event of a disruption, and what the level of tolerance would be for data not being available;

3

Establish a prioritized list of government services for cloud migration.

In addition to understanding what data should be considered essential in terms of cyber resilience, governments should consider prioritizing their various government services and databases as critical to the functioning of the government. This perspective should incorporate a wider selection of services than those already identified under "critical", "vital", or "essential" services, upon which life and well-being depend. These services should include information systems where unavailability for any significant period of time would be unacceptable, for example land or tax records.

4

Implement pilot projects to test established technical and policy requirements for use of cloud computing in the public sector.

Governments, regions, and cities should partner with the industry to develop and implement pilot projects to address any concerns or unanswered questions they might have. Pilot projects could look to deepen the understanding of cloud computing technology, test specific crisis scenarios, or seek to address a particular security concern the organization might have. The partnership with the private sector will allow governments to leverage their own experts, and to harness technical and product specialists that might have seen similar scenarios elsewhere.

5

Update public policy, as needed, to enable the use of cloud computing for cyber resilience.

Policies that predate cloud computing sometimes inadvertently erect barriers to its adoption, in particular in the public sector. Whilst it is critical that governments put appropriate safeguards in place that ensure the security and protection of their data, the data of their citizens, as well as their services, these must be proportionate to the risks faced. Cloud security has evolved substantially in recent years and cloud can therefore often provide significantly improvements on the security of technologies organizations have in place on premise. Cyber resilience benefits can be particularly large.

6

Develop the technical process of migrating data and services to the cloud.

Critical to any successful migration of data and services to the cloud, as well as to digital continuity, is developing and understanding the processes and procedures that govern it. These should, amongst other things, include understanding what type of data has been approved for migration, and addressing how failover of particular government services to the cloud should be managed. These need to be agreed upon ahead of the process beginning, to be documented, and to be be repeatable.

7

Rely on established best practices for proof of efficacy of security practices in place.

Public sector organizations continue to view cloud computing with a level of concern, as its adoption is often perceived as loss of control. To address this challenge, we recommend governments adopt international security standards as part of their procurement processes to help them better understand how vendors manage security in their products and services. Moreover, we encourage them to require appropriate proofs of the efficacy of security capabilities in place.

8

Conduct regular reviews of the policies and process in place.

To be able to effectively respond to the evolving cybersecurity threat landscape, governments need to ensure that they continuously monitor their risk environment and conduct regular risk assessments and cybersecurity exercises. Additionally, they should also frequently assess new technologies on the market to determine whether these can support their cyber resilience efforts. In line with this, policies and procedures must be re-evaluated to adapt and support pragmatic use of such innovations.

Conclusion

Governments, irrespective of their size or location, will sooner or later experience a crisis scenario involving cyber resilience and digital continuity, given the increasing levels of technology use and connectivity across all aspects of economic, social and bureaucratic activity and society. Resilience and continuity will be important not only when it comes to crises directly affecting a nation, region or city but also when dealing with the ripples and collateral effects that affect our globally interdependent cyber infrastructure and systems.

Whether it is by considering cloud migration for greater cyber resilience, or committing to digital continuity for government services, governments and public sector organizations in general should view cloud computing as an important tool in shoring up their crisis management plans and capabilities.

Challenges to fully embracing this technology remain, however. These are not primarily technical; most on-premise applications in place today allow for what is a fairly simple shift, although the transition needs to be carefully planned and executed. The essential challenges are ones of perception and of policy.

To ensure that cloud computing can be used for cyber resilience, many existing legislative and policy frameworks require a review. The key legal and political issue is very likely to be the transfer of certain classes of data across national borders. Furthermore, given the rapid pace of technological developed, even updated, outcome-focused legal frameworks will require regular revisiting in order to enable an appropriate and secure use of cloud. Beyond this, it will be essential to create trust-based partnerships between government actors and private sector cloud providers.

The reward for states, regions and cities that embrace the cyber resilience prospects afforded by cloud computing and that overcome the policy and technical challenges faced will not be limited to safeguarding the operability and continuity of their essential functions and services. The wider opportunities of the technology for public and private sectors, from government agencies to start-up entrepreneurs, will be all the easier to embrace thanks to the supportive legal and policy framework that will result from this process.

Annex: Essential questions to be asked

To help governments and public sector entities assess the utility and practicality (technical and legislative) of using cloud computing for advancing their cyber resilience plans, Microsoft has developed the following questionnaire. The questions seek to provide organizations with assurance regarding security practices that the cloud vendor has in place, as well as to help guide assessments of cyber resilience and readiness. We recommend that these questions are utilized not as part of a procurement exercise, but deliberated upon in partnership with cloud vendors as part of pilot projects.

Assessing threats and vulnerabilities.

- What cyberthreats, natural disasters and other threats are of primary concern?
- What are the respective probabilities and consequences of these threats, notably their impacts on government services and citizens?
- What technologies and processes are in place to help detect, prevent and counter these threats?
- What technologies and processes are in place to maintain and restore government services in the face of these threats?
- How do you access and test your technologies and processes?

Prioritizing critical services

- What is the hierarchy or classification of critical services that need to be protected most and recovered first?
- What form(s) of resilience and continuity plans are currently in place for these services?
- Do these plans align with the latest assessments of threats and capabilities?
- What are the ideally desired resilience and continuity outcomes for these critical services?
- It terms of optimal outcomes, how long can these critical services be offline and how can this be described in terms of Recovery Time Objectives (RTOs) and Recovery Time Capabilities (RTCs)?

Assigning roles and responsibilities

- Has a chief (cyber) resilience officer been appointed? Is there an individual or team with responsibility for digital continuity issues?
- Who is responsible for the ICT risk registry and does it span physical and ICT infrastructure?
- Has a coordination center that brings together incident response, legal, public relations, public safety, and other relevant stakeholders been implemented?
- Is there a dedicated cyber-resilience budget?
- How is the effectiveness of the cyber resilience plan measured?

Understanding the domestic legislative environment

- What type of data, if any, can be migrated to the cloud?
- What policies exist or need to be created to allow for cross-border transfers of government-held data identified as needing to be migrated to the cloud as part of resilience of continuity planning?
- Do government policy frameworks and standards need to be updated to specifically address the use of cloud computing for cyber resilience?
- Which policy areas are involved, e.g. data protection, data classification, and security?
- Should there be a requirement for a defined geographic failover capability, which provides protection against a state's, region's or city's infrastructure being severely impaired by man-made or natural disasters?

Partnering for cyber resilience

- Does commercially developed and provided cloud have a viable and practical role in protecting and recovering critical government services, systems and data?
- Can the government or public sector organizations leverage general partnerships with private companies to help meet resilience and continuity goals and objectives?
- Can partnerships with other governments or inter-governmental organizations help with resilience and continuity?
- Is there a process in place to encourage a broader discussion on resilience and continuity with citizens, industry and non-governmental organizations to identify opportunities for improvement?
- What additional assurance mechanisms need to be developed to ensure public trust in cloud computing?

Assessing the security of your cloud provider (policy)

- Who can access and use the data in the cloud?
- Where is the data stored?
- Can the data be retrieved and moved to a different provider if needs be?
- What data privacy and security controls does the cloud vendor have in place?
- What are the cloud provider's service uptime commitments and capabilities?

Assessing the continuity capabilities of your cloud provider (technical)

- Will government services be able to continue to perform their essential functions in the cloud?
- Is it practical for existing platform architectures, originally developed to run on-premises, to be optimized to support cloud platforms?
- How significant will architectural changes to the existing applications need to be in order to support failover or migration to the cloud?
- Will modification of procedures for on-premises failover and fail-back be required?
- Can acceptable recovery time objectives (RTOs) be achieved?