Essential role of cloud computing in cyber resilience and digital continuity

Societies around the world are being reimagined and challenged by emerging technologies such as artificial intelligence, big data and the Internet of Things. As government operations become more data-driven and technology-centric, they need to be made as resilient as possible, not only to cyber-threats but to the wider range of natural and man-made disasters that can occur.

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 their services rapidly. In other words, for governments at the national, regional or city level cyber resilience ensures that its 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 an organization can develop its resilience. Its purpose is to maintain digital services and data relevant for the functioning for those services, regardless of any adverse changes or interruptions. Digital continuity is about an information technology system’s ability to continue delivering as intended, even if cybersecurity is failing or has failed.

However, that is easier said than done. Even before the focus shifts to one of continuous learning and reinvention - the essential part of resilience - one of the major challenges is accurately characterizing and quantifying the core capabilities needed. This work includes: i) identifying key threats and assess their impact on critical systems and functions; ii) classifying and prioritizing critical services; iii) setting cyber-resilience goals and objectives; iv) developing desired cyber-resilience outcomes and identifying and test capabilities; and v) defining roles and responsibilities and determining the resources needed.

Cloud computing benefits

When it comes to continuous adaptation and reinvention, 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. For example, a key feature of cloud computing is the type of 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. Moreover, 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. Because certain government data and services are likely to be in particularly high demand during times of crisis, the highly scalable nature of cloud computing means systems supporting these services are less likely to crash, even under unusually heavy usage requirements.

Components of cyber resilience

1. 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.

2. 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.

3. 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...
Essential role of cloud computing in cyber resilience and digital continuity

Furthermore, cloud vendors recognize that trust is a fundamental part of their business model and do their utmost 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.

Adopting a cyber resilient posture

An effective and cyber-resilient implementation of cloud computing services requires public sector entities to adopt 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. Conduct a threat analysis.
2. Classify and prioritize critical services.
3. Set cyber resilience goals and objectives.
4. Implement pilot projects to test established technical and policy requirements for use of cloud.
5. Set cyber resilience goals and objectives.
6. Define roles and responsibilities and determine resources needed.
7. Conduct regular reviews of the policies and process in place.

Governments, irrespective of their size or location, will sooner or later experience a crisis scenario involving cyber resilience and digital continuity. Resilience and continuity will be important not only when it comes to crises directly affecting an organization, 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.

However, to ensure that cloud computing can used for cyber resilience, many existing legislative and policy frameworks require a review, which is likely to be complex and will identify issues of controversy, such as what kind of data is allowed to be transferred across national borders. Nevertheless, the reward for states, regions and cities that embrace the cyber resilience prospects afforded by cloud computing and 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.