# Using a Data-Centric Approach to Reduce Risk and Manage Disruption

*How can organizations step up their data privacy and compliance programs to weather current and future disruption?* ***Paul Agbabian****, global CTO and chief architect for Symantec Enterprise Division of Broadcom, makes the case for a data-centric approach.*

***How do new privacy regulations and the evolving definition of privacy impact computing and network infrastructure?***

They have a major impact because key concepts of privacy law — the need for justification to process the data, data minimization, the right to be forgotten and purpose specificity, to name a few — regulate how organizations can collect and process data. Therefore, infrastructures must be able to give them the data they need for their use cases while remaining in compliance with their regulatory obligations. In addition, privacy laws extend to cloud, SaaS-based services and other hosted technologies where the organization's regulated data may exist.

***How has the massive shift to telework and hybrid work scenarios impacted data privacy and compliance?***

We see a couple of major shifts and risks. Teleworking has demonstrated the elasticity of traditional perimeter defenses. Now, the enterprise environment needs to extend into the home of every employee who works remotely, and it must protect sensitive data on their machines from attacks and breaches. To do so, the organization has to monitor and collect a massive amount of data flowing in and out of these devices. That data can be used for security but also for other purposes such as performance management or contact tracing. This potentially turns devices into information sources for an employee's location and offline interactions, leading to mass surveillance risks if the data is ever abused.

***Please explain a data-centric approach and how it helps simplify data privacy and regulatory compliance.***

A data-centric approach is about being able to understand how data flows and being able to enforce policies and procedures on the data, based on its sensitivity and perceived risk. It's much more effective to associate policy and controls with a data set that we know contains sensitive data as opposed to applying policies on a particular device. Devices can be an important control point, but the sensitivity and risk is related to the data, and it's the data that needs to be protected across its life cycle, regardless of where it's located.

***What early steps should agencies take to ensure compliance and manage the costs associated with it?***

It's critical to embed privacy and security considerations early in the design phase of their infrastructure and architecture. Regulatory requirements are constantly changing and they vary by jurisdiction, so you can't design in a way that's targeted too closely to any one particular regulatory framework. It's much easier to manage these things if privacy and security are built in from the beginning and are not an afterthought. Doing so allows for a holistic governance framework and enables organizations to manage risks and costs because they can calibrate compliance and governance to their particular requirements and use cases.

***What should agencies watch for as they adopt artificial intelligence and machine learning to streamline data privacy and compliance?***

AI and ML have a lot of potential to streamline privacy and compliance, but they also come with certain risks. For example, AI/ML require systems to be trained. If systems are trained inadequately or with inaccurate data, the result may be poor decisions that ultimately cause more damage than good. This is why, as discussions about the use of AI and ML continue, we expect to see more emphasis on accountable development and usage. In practice, this means having requirements around transparency of AI usage, decisions and data quality, as well as robustness in terms of AI security and resilience.

***What advice can you give agencies as they modernize and extend their infrastructures to adapt to "the new normal" and future disruptions?***

Disruptions are the new normal. They can be cyberattacks, natural disasters, geopolitical tensions, a pandemic like the one we're experiencing now or the deployment of a disruptive technology like quantum computing. Organizations must expect this new reality and prepare for it by having a consistent governance framework, flexible yet robust cybersecurity and resilience, and a strong understanding of their data flows and data usage. These capabilities enable them to adapt to whatever new disruption may come around the corner.

# Empowered Citizens. Efficient Agencies.

## Delivered with a proven, modernized IT environment.

Welcome to the era of the integrated and agile IT environment. An environment where your government agency is equipped for a future of **increased visibility**, trusted access to services and more streamlined operations — **just the way you operate**. It's an environment where mobile-to-mainframe agility, data access and data protection come together like never before allowing you to balance the needs of implementing new services and updating existing services easily and quickly.

Talk to us about your mission to modernize at **www.broadcom.com/ca-software**

BROADCOM®