


Characteristics of Human Elements Focused on Data, Threats, Risk, and Privacy Management for Smart Cities

Yakubu Ajiji Makeri, Kampala International University, Uganda*

 <https://orcid.org/0000-0002-8325-8845>

ABSTRACT

In numerous nations, laws have not kept up with the innovation, leaving critical holes. In different nations, law implementation and insight offices have been given critical exceptions. At last, without sufficient oversight and implementation, the simple presence of a law may not give satisfactory protection. The expanding complexity of data innovation with its ability to gather, dissect, and spread data on people who have acquainted a desire to move quickly with the interest for enactment. Moreover, new improvements in clinical exploration and care, broadcast communications, progressed transportation frameworks, and monetary exchanges have significantly expanded the degree of data produced by every person.

KEYWORDS

Data, Government, Security

INTRODUCTION

Innovation has become a significant device for some non-administrative associations (NGOs) and gatherings gathering information in the creating scene. For instance, innovation can furnish individuals in far-off districts with admittance to monetary administrations and permit associations to gather crucial data inside the networks they serve. Data and Communication Technology for Development (ICTD) is the investigation of what innovation can achieve and how innovation is utilized in such low-asset settings around the globe. ICTD takes a wide meaning of “low-asset”. Regions influenced by destitution are often the focal point of ICTD, yet any setting where things like restricted network, problematic force, or daintily gifted staff scheme to make a novel mechanical scene may be pertinent to ICTD. Even though there have been a few endeavors to study and address PC security and protection chances with advances in an ICTD climate, both dependent upon the situation for explicit innovations and from a scholastic viewpoint, e.g., (Ben-David et al., 2011, Corrigan-Gibbs and Chen, 2014, Reaves et al., 2015), the space of “PC security meets ICTD” is as yet in its outset. We add to this space through bits of knowledge into how to assess and address PC security chances in ICTD

DOI: 10.4018/IJSST.297924

*Corresponding Author

conditions. To give an establishment to our bits of knowledge, we decide to zero in on a specific class of advancements—information assortment toolbox—and, specifically, a particular, generally utilized occasion of such an innovation: Open Data Kit (ODK). Information is critical for some NGOs and analysts to screen and assess arrangements or mediations and report to givers on exercises. For instance, associations may gather persistent data during center visits, evaluate the commonness of irritations in-country farmland, or report a foundation needing a fix. ODK permits computerized structures to be made without profoundly specialized aptitude, and has been utilized as a stage by various associations. By considering PC security chances with ODK, we can extricate exercises for both ODK and other information assortment arrangements, just as construe exercises for other new ICTD advances.

BUILD UP DATA SHARING OBJECTIVES AND TARGETS THAT HELP BUSINESS CYCLES AND SECURITY APPROACHES

An association's data sharing objectives and goals should propel its general network safety methodology and help an association with all the more successfully oversee digital-related danger. An association should utilize the consolidated information and experience of its faculty and others, for example, individuals from digital danger data sharing associations, to share danger data while working per its security, protection, administrative, and lawful consistence prerequisites.

DISTINGUISH EXISTING INTERIOR WELLSPRINGS OF DIGITAL DANGER DATA

Associations ought to distinguish instruments, sensors, and vaults that gather, produce, or store digital danger data, danger investigation stages, and conveyance instruments that help the trading of digital danger data. As inside digital danger data sources and abilities are distinguished, associations ought to decide how data from these sources at present help online protection and hazard the board exercises. Associations ought to likewise archive noticed information holes and consider procuring extra danger data from other (conceivably outer) sources or through the arrangement of different instruments or sensors. At last, associations ought to distinguish dangerous data that is accessible and reasonable for imparting to outside gatherings.

DETERMINE THE EXTENT OF DATA SHARING EXERCISES

The expansiveness of an association's data sharing exercises should be steady with its assets, capacities, and destinations. Data sharing endeavors should zero in on exercises that give the best incentive to an association and its sharing accomplices. The perusing action ought to distinguish kinds of data that an association's key partners approve for sharing, the conditions under which sharing of this data is allowed, and those with whom the data can and should be shared.

SET UP DATA SHARING GUIDELINES

Sharing guidelines are expected to control the distribution and conveyance of dangerous data, and thusly help to forestall the dispersal of data that, if inappropriately revealed, may have unfavorable ramifications for an association, its clients, or its colleagues. Data sharing rules should mull over the dependability of the beneficiary, the affectability of the mutual data, and the possible effect of sharing (or not sharing) explicit sorts of data.

9 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/article/characteristics-of-human-elements-focused-on-data-threats-risk-and-privacy-management-for-smart-cities/297924

Related Content

Adding Context Information to Video Analysis for Surveillance Applications

Solmaz Javanbakhti, Xinfeng Bao, Ivo Creusen, Lykele Hazelhoff, Willem P. Sanberg, D.W.J.M. (Denis) van de Wouw, Gijs Dubbelman, Svitlana Zingerand Peter H.N. de With (2017). *Biometrics: Concepts, Methodologies, Tools, and Applications* (pp. 1656-1700).

www.irma-international.org/chapter/adding-context-information-to-video-analysis-for-surveillance-applications/164670

Image Quality Assessment and Outliers Filtering in an Image-Based Animal Supervision System

Ehsan Khoramshahi, Juha Hietaoja, Anna Valros, Jinhyeon Yunand Matti Pastell (2017). *Biometrics: Concepts, Methodologies, Tools, and Applications* (pp. 1241-1257).

www.irma-international.org/chapter/image-quality-assessment-and-outliers-filtering-in-an-image-based-animal-supervision-system/164647

Beyond Communication and Control: Environmental Control and Mobility by Gaze

Richard Bates, Emiliano Castellina, Fulvio Corno, Petr Novákand Olga Štěpánková (2012). *Gaze Interaction and Applications of Eye Tracking: Advances in Assistive Technologies* (pp. 103-127).

www.irma-international.org/chapter/beyond-communication-control/60037

Detecting Facial Expressions for Monitoring Patterns of Emotional Behavior

Nikolaos Bourbakis (2013). *International Journal of Monitoring and Surveillance Technologies Research* (pp. 1-28).

www.irma-international.org/article/detecting-facial-expressions-for-monitoring-patterns-of-emotional-behavior/93051

Hybrid Data Mining Approach for Image Segmentation Based Classification

Mrutyunjaya Panda, Aboul Ella Hassanien and Ajith Abraham (2017). *Biometrics: Concepts, Methodologies, Tools, and Applications* (pp. 1543-1561).

www.irma-international.org/chapter/hybrid-data-mining-approach-for-image-segmentation-based-classification/164663