ESSAY

Computer Sciences & Information Technology

Cybersecurity for Open Data

Name of the Student

Name of the Institution

The United Nations General Assembly in 1946 recognized freedom of information as a fundamental right of freedom. Article 19 of the 1948 Universal Declaration of Human Rights further identified this right as an integral part of human rights and freedom (Assembly, 1948). The 21 st Century is characterized by increased tremendous technology growth, which facilitates fast and efficient dissemination of (and access to) information. This is also accompanied by need for efficiency, transparency, freedom and democracy, and governance. As a response to these needs, governments, and business organizations resorted to using open data that eases access and use of information. Government agencies release large data sets online, which are freely accessible by the online society (Ayre & Jim, 2017). This data can be analyzed, reused, and redistributed at no cost.

Open data, therefore, refers to data that is collected and shared without usage and copyright restrictions. This data is mostly unclassified and is devoid of personally identifiable data (PID). This implies that open data is & 39; legally open& 39; and can, therefore, be legally shared and used by individuals, researchers and organizations without minding the restrictive nature of copyright terms (Smith & Johan, 2018). Examples of data that have been traditionally distributed as open data include postal codes, weather, and crime reports among others. The internet is a major driving force that helps in the collection and free distribution of data. Open Data distribution in the United States of America started in the 1970s when the National Oceanic and Atmospheric Administratio n began to release weather forecast data to the masses. President Obama&39;s administration further in 2013 reinforced the state of open data through the machine Readable Open Information executive order. Unlike open records that must. be procedurally accessed, open data includes declassified information that is availed to the public when they cease from being sensitive to national security (Okamoto, 2017). This makes sharing and usage of such data risk-free.

Benefits and Value for Open Data

Open data has tremendous potential for creating economic value for companies and businesses. This is realized through the diverse application of open data as provided by Group on Earth Observation (GEO). The GEO is an agency that advocates for open data and envisions a future in which decisions affecting "humankind are influenced by well-coordinated and comprehensive earth observations and data (Melin, 2016)." Through the GEOSS portal, business organizations get access to voluminous data and that which can be effectively mined to provide business insights. Such data can be used to reach and sustain clients, improve brand quality, and enhance overall organizational performance. A 2000 report recorded that through the weather satellite sector open data policy helped in the formation of about 400 organizations, and produced $400 to $700 million in gross receipts besides creating employment opportunities for over 4000 American citizens (GEO, 2015). Traditional data access policies required teams of employees to draft, implement, and apply rules and regulations about data access. However, with open data, such organizations only require one staff or none at all-where operations are fully automated. Open data policy also enhances social welfare. By readily availing information to citizens, GEO helps them make sound decisions that improve quality of life. Data received from such agencies as GEO help individuals understand their environments better. Such information is crucial in the development of a secure, healthy, and educated nation (Schrier, 2014). These benefits can only be realized when data is made freely accessible to citizens at all times. Other societal benefits of open data include meeting requirements for access to information in the digital, promoting reputational benefits, and implementing ethical principles.

Open government data helps create transparency and accountability, thus preventing fraud. Policies governing open data suggest that such financial information as donation targets and tax dollar spending be availed to the public for scrutiny purposes. Such data can be compiled and analyzed, leading to the making of such decisions as reducing national workloads. Additionally, government employees are forced to be accountable since they are always expected to ascertain government expenditure.

Security Concerns

While releasing data helps increase transparency in governance by allowing citizens to engage their governments actively, it usually comes with some tradeoffs. Open data typically contain information about people, and releasing it to the public compromises their privacy rights. Although open data policies emphasize the usage of data that is devoid of personally identifiable information, sophisticated tools can be used to reverse-engineer this data, thus revealing its subjects. Additionally, several pieces of information can be compiled together to give ‘helpful’ insights that can be used to identify an individual. Open government data requires that all information shared be of high quality, factual, authentic, and high integrity 'value.' Any data that does not meet these requirements cannot be used to make sound decisions; neither can it be of any significance to its owner. Open government data is required to be complete and consistent. The principle of free use, re-use, and dissemination expose data to cyber attackers who can edit for their gain. Third parties too have access to open data. Maliciously-intended persons can use

such information to launch cyber attacks. Readily available data can be used to create access to restricted data. Once access is created, the availability of critical government services can easily be affected.

The USA government uses various means to regulate the access to and usages of open data by using NIST's security framework. This framework provides ways through which data is released to the public and suggests that data be thoroughly reviewed before publishing it to the public. The government introduces slight changes to files with names or personally identifiable information to protect such individuals. This approach also ensures that criminal generalization is based on a section of a city or both.

Best Practices

The best practice for open data would be ensuring that data is correct, complete, factual, authentic, and consistent. Adherence to NIST's guidelines when compiling and publicizing data helps 'produce' data that meet these criteria. Additionally, it helps meet the integrity and data authenticity requirements. The framework also ensures that such data contains no PID by removing and properly disposing of all personally identifiable information (Force, Joint Task, and Transformation Initiative, 2013). It is also a way of ensuring that the federal Privacy and Economic Acts are followed when publishing data online and that only the required data is released. It is also a way of ensuring that critical information pertinent to the main body is not left out during the publication. Adherence to the 1974 Privacy Act would ensure that companies and government agencies do not expose themselves to cyber attacks or legal actions sanctioned against them, mainly due to negligence.

Summary

In conclusion, the 21st Century is characterized by tremendous growth in technology. The information age, on the other hand, is characterized by data and data processing that form the core of business operations. Any data that is devoid of PID, restrictive copyright requirements, and that which is legally free is called open data. The development of open data has great benefits to governments, business organizations, and citizens as well. Readily available information is crucial for the making of critical decisions and strategic planning in business organizations. Through this data, organizations enhance their customer service, performance, and productivity while reducing operational costs. Governments increase transparency and democracy by allowing citizens access to government information. This, in turn, reduces fraud and increases accountability. Individuals are in a position of making informed decisions that improve their living standards thanks to open data.

Nevertheless, open data is subject to privacy, integrity, and availability concerns. With present-day technologies, it is possible for individuals to reverse engineer this information and to compile various datasets to reveal the privacy of persons. The correctness, consistency, and completeness of such data are also a major concern. Releasing too much information is also hazardous in that hackers can use this information to gain access to the restricted data. The NIST cybersecurity framework gives guidelines on how open data is collected, compiled, and publicized. It suggests that any data be reviewed for any PID, incompleteness, inconsistency, and accuracy purposes. Adhering to this recommendation, in addition to Privacy and Economic Acts as enacted by the Federal governments, is the best practice for ensuring non-repudiation open data security.

References

Assembly, U. G. (1948). Universal declaration of human rights. UN General Assembly, 302(2).

Ayre, L. B., & Craner, J. (2017). Open data: What it is and why you should care. Public Library Quarterly, 36(2), 173-184.

Force, Joint Task, and Transformation Initiative. (2013). Security and privacy controls for federal information systems and organizations. NIST Special Publication, 800(53), 8-13.

GEO. (2015, November 13). The Value of Open Data Sharing. Retrieved February 02, 2020, from Group on Earth Observations: https://www.earthobservations.org/documents/dsp/20151130_the_value_of_open_data_sharing.pdf

Melin, U. (2016, August). Challenges and Benefits in an Open Data Initiative–Local Government Case Study of Myths and Realities. In 15th IFIP Electronic Government and the 8th Electronic Participation Conference (EGOV ePart 2016) (Vol. 23, pp. 111-122).

Okamoto, K. (2017). Introducing open government data. The Reference Librarian, 58(2), 111-123.

Schrier, B. (2014). Government open data: Benefits, strategies, and use. The Evans school review, 4(1), 12-27.

Smith, G., & Sandberg, J. (2018). Barriers to innovating with open government data: Exploring experiences across service phases and user types. Information Polity, 23(3), 249-265.