The Safety of Cloud Computing: An Annotated Bibliography

Amaya Shepard

English 132: Information Literacy and Research

Dr. Victoria Batten

September 24, 2020

Brodkin, J. (2017, July 02). Gartner: Seven cloud-computing security risks. Retrieved August 29, 2020, from https://www.infoworld.com/article/2652198/gartner--seven-cloud-computing-security-risks.html

Written by Jon Brodkin of Network World, this article addresses numerous staggering issues with the security of cloud computing, in which most users don't discern. For example, one of the least well-known facts about cloud computing mentioned in this article is the user is ultimately responsible for the security and integrity of their data, regardless of hosting it in the cloud with "secure" providers. The explicit audience would be cloud computing service providers, and the implicit audience is users of said cloud computing service." Encryption is effective but isn't a cure-all," stated Brodkin. An additional issue presented in the article is that investigating data in the cloud could be nearly impossible. Data for a user may be located and hosted in various locations worldwide, and that data is not stagnant; it is always being transferred to other data centers. If your information were to be lost, it could take a substantial amount of time for the cloud service provider to investigate the transmission of your data, and even longer to recover it. Brodkin presents vastly pertinent issues with cloud computing, and for this reason, this article is a good source of information for my research.

Chou, T. (2016). Security Threats on Cloud Computing Vulnerabilities. Retrieved September 22, 2020, from http://airccse.org/journal/jcsit/5313ijcsit06.

Te-Shun Chou, of East Carolina University's Technology Systems Department, has written an in-depth article about the risks of storing data in the cloud and how hackers use security

vulnerabilities to steal personal information. Early in the article, Chou focuses on the mass use of cloud storage and the variety of abused security vulnerabilities in which confidential information is stolen, and either stolen or used for various other e-crimes. The targeted explicit audience would be those who indulge in cloud usage, and the targeted implicit audience would be Cloud Computing companies. Chou's primary argument argues that while cloud computing is widely-used and accepted, your information is at risk each time a hacker presses a vulnerability in the cloud's architecture, which leads to data leaks. Hackers employ various techniques to gain access to clouds without legal authorization or disrupt services on clouds to achieve specific objectives. Chou even explains the most common method hackers deploy, in which hackers use session tokens and "trick" the cloud into thinking their illegal activity is a valid, authorized instance. The evidence used for Te-Shun Chou's studies are factual and verifiable, due to the sheer fact of using publicized, researchable statistics for data-leaks due to said security vulnerabilities. This article is an excellent addition to my research, as it uncovers various secondary breach tactics and provides accurate statistics.

Heiser, J., & Nickolett, M. (2019, June 03). Assessing the Security Risks of Cloud Computing. Retrieved September 24, 2020, from https://www.gartner.com/en/documents/685308/assessing-the-security-risks-of-cloud-computing.

Written by Jon Heiser and Mark Nickolett, Assessing the Security Risks of Cloud Computing discusses the associated security risks of cloud computing. The focused topic identifies and evaluates several vulnerabilities in many facets of various components of Cloud Computing. From a security and risk perspective, it is the least transparent

externally sourced service delivery method, storing and processing your data externally in multiple unspecified locations, often sourced from other, unnamed providers, and containing data from numerous customers. The targeted explicit audience would be cloud users, and the implicit audience would be cloud computing service companies. The article addresses various security vulnerabilities. When addressing Privileged User Access (PUA), when sensitive data is processed outside the enterprise, or by non-employees, it means that organizational managers are less immediately aware of the nature and level of risk and that they have no direct ability to control these risks. When addressing compliance and user-agreement, most regulations hold the user of the service ultimately responsible for the security and integrity of their corporate and customer data, even when the service provider has it. Heiser and Nickolett back their arguments with publicized statistics and published agreements, such as EULAs and user-agreements. Therefore, this article is an excellent addition to my research on the safety of cloud computing.

Carlin, S. (2013). Cloud Computing Security. In 944984535 737840089 K. Curran (Author), Pervasive and ubiquitous technology innovations for ambient intelligence environments (Vol. 1, pp. 195-201). Hershey, PA: Information Science Reference.

The author of the Cloud Computing Security chapter in Pervasive and Ubiquitous Technology Innovations (abbrev.), Kevin Curran outline what cloud computing is, the various cloud deployment models, and the main security risks and issues that are currently present within the cloud computing industry. Curran speaks diligently about the vast dangers of cloud computing and how they could be avoided. The explicit audience would be cloud users, and the implicit audience is cloud service providers. The focused topic of this chapter is the risks of data leaks due to poor security and security measures that should

be implemented to better the protection of data and services. The author uses publicized and verifiable statistics, in addition to EULAs and user-agreement statements. This source appropriately employs legitimate data to back its' arguments and will be a great addition to my research on the overall security of Cloud Computing.