Annotated Bibliography

Carr, Ramona. “Top Challenges in Cloud Security for 2018.” *Zettaset*, 29 Mar. 2018, www.zettaset.com/blog/top-challenges-cloud-security-2018/.

From a more technical perspective, the author, Ramona Carr, discusses some of the risks of cloud storage. He mentions Denial of Service (DoS) and the hardware vulnerabilities found in microprocessor architecture known as Spectre and Meltdown. Attacks of these nature can affect most devices in service today, ranging from cellphones, laptops, and even servers, which is where cloud storage is hosted. He discusses the number of data breaches that occur across numerous sectors and strongly recommends the use of cloud encryption solutions to combat this issue.

Shaw, David. “Top 5 Cloud Storage Security Challenges.” *Nasuni*, 31 Aug. 2018, www.nasuni.com/top-5-cloud-storage-security-challenges/.

The author of this article, David Shaw, discusses some of the issues that companies face with implementing cloud solutions. By implementing cloud solutions, the possibility of a data leak increases, which is why a company should never rely on the cloud service provider solely for encrypting their data. The author also discusses how a company’s cloud credentials are handled. It’s possible that multiple companies may receive similar credentials from the service provider and create the possibility of unintended access.

Morrow, Timothy. “12 Risks, Threats, & Vulnerabilities in Moving to the Cloud.” *SEI Insights*, 5 Mar. 2018, insights.sei.cmu.edu/sei\_blog/2018/03/12-risks-threats-vulnerabilities-in-moving-to-the-cloud.html.

The author, Joy Ma, discusses additional vulnerabilities of cloud computing in relation to the application programming interface that cloud providers give to their customers to interact with their servers. These APIs, like any other code, is susceptible to vulnerabilities and it’s possible for a user to gain access to a company’s network, the stored data, or the cloud provider’s infrastructure. The author also discusses the possibility of incomplete data deletion. Since data is often stored across numerous devices and in different formats, it’s possible that data is not completely deleted when requested, and so the remnants may provide information to an outsider.

Ma, Joy. “Top 10 Security Concerns for Cloud-Based Services.” *Incapsula.com*, 14 Dec. 2015, www.incapsula.com/blog/top-10-cloud-security-concerns.html.

This article discusses issues related to information being leaked by insider sources. Depending on permission management, its possible that data could be accessible by employees that should be confidential. This means that someone can intentionally or unintentionally gain access to the data. Also, because cloud services tend to operate across many devices, the author discusses the possibility of someone hijacking someone else’s account to gain additional permissions.