There are always threats that the Burdell Bank will have to deal with. By switching to the cloud, there are some threats that are more prevalent in the cloud than within our past practice. These include misconfigurations, insider threats, hijacking accounts, and network threats.

Misconfigurations are commonly exploited vulnerabilities in cloud infrastructures which can be exploited for various threats. Misconfigurations are particularly dangerous because of their potential to leave cloud-based systems and data exposed to bad actors. In a cloud environment, misconfigurations can allow attackers to gain unauthorized access to sensitive data, compromise applications, and even take control of the cloud infrastructure. For example, a misconfigured firewall rule may allow unauthorized traffic to access a cloud-based database, exposing sensitive data to attackers. Similarly, misconfigured user permissions may allow attackers to escalate privileges and gain access to confidential information. Cloud environments are dynamic, complex, and have multiple users and applications accessing resources at any given time. This complexity not only makes it challenging to properly configure and manage the system, but it also allows misconfigurations to go undetected for extended periods of time [1]. Through exploiting misconfigurations, attackers can cause significant damage to an organization and its clients before remediation. A comprehensive and proactive approach is necessary to mitigate this threat.

Insider threat is one of the key concerns enterprises and individuals have regarding cloud computing. Putting data in the cloud increases the number of people with access to the data, which may increase the risk of insider attacks [2]. However, safeguarding data on the cloud against an organization's insiders may necessitate new mechanisms distinct from those employed to protect locally stored data [2]. In the event that an employee gains unauthorized access to our cloud-based systems or data, there is a possibility that the consequences will be severe. These consequences may include the theft of data, the loss of intellectual property, and damage to our reputation. Workers that violate security policies and protocols should be punished with penalties up to and including termination from their positions. Our mission is to maintain the privacy and safety of our information systems, as well as the trust of our clients and other commercial associates.

Hijacking accounts is another one of the key threats to cloud computing. This can be done in multiple different ways including social engineering or weak password protection. While these types of threats also occur in on-premises environments, they are a bigger issue within cloud infrastructures These threats occur in both the cloud and on-premises, but organizations generally cannot identify and respond to these threats in the cloud as well as they can on-premises [3]. Threat actors gaining access to accounts lets them gain access to sensitive information and software. This could result in theft, fraud, or identity theft. Threats regarding hijacking accounts are especially hard to stop since the cause is usually from human error as opposed to technical issues. This means that there needs to be good policy to help prevent this type of threat.

Network-based threats to cloud security can cause significant damage to organizations. Network attacks are any unauthorized attempts to disrupt, damage or gain unauthorized access to a computer network or system. Distributed Denial of Service is a common network attack. A DDoS attack uses a network of multiple devices or computers, also known as a botnet, to flood an organization’s network and servers [4]. This can cause services to become unavailable to legitimate users leading to lost revenue, reputational damage, and customer dissatisfaction. Attackers also aim to exploit vulnerabilities in an application’s code. A code injection attack involves an attacker injecting malicious code into an application’s input field [4]. The application

processes the input without proper validation or sanitization, allowing the attacker's code to execute and gaining unauthorized access to application. This can lead to sensitive data being stolen or deleted.

A comprehensive and proactive approach is necessary to mitigate these types of threats. While these threats are more concerning in cloud computing, we still need to take other threats into account. Therefore, these are generally the most concerning within cloud computing.

References

[1] Waqas. “QR Code Generator MY QR Code Leaks Users' Login Data and Addresses.” HackRead, February 19, 2023. https://www.hackread.com/qr-code-generator-my-qr-code-data-leak/?web_view=true.

[2] A. Mahalle, K. Yong, and X. Tao, “Insider threat and mitigation for cloud architecture ... - IEEE xplore,” IEEE Xplore, 2019. [Online]. Available: https://ieeexplore.ieee.org/document/8791906/. [Accessed: 15-Mar-2023].

[3] “Top Cloud Security Issues, Threats and Concerns.” Check Point Software. Check Point Software, July 15, 2022. https://www.checkpoint.com/cyber-hub/cloud-security/what-is-cloud-security/top-cloud-security-issues-threats-and-concerns/.

[4] “Network Attacks and Network Security Threats.” Cynet, January 6, 2023. https://www.cynet.com/network-attacks/network-attacks-and-network-security-threats/.