As businesses increasingly rely on Amazon Web Services (AWS) for their cloud computing needs, it becomes vital to understand the potential risks associated with its usage. Specifically, the proper administration of AWS's Identity and Access Management (IAM) is crucial in ensuring the security of these digital assets. IAM's primary role is to manage users and their access to AWS resources, but its misconfiguration can be a notable vulnerability.

One of the most common pitfalls is the misconfiguration of permissions. Unintended permissions, either too lax or too extensive, can expose critical data and resources to unwarranted access. When IAM is not accurately set up, entities can gain more access than intended, leading to potential data breaches, financial loss, or even infrastructure sabotage. The ramifications of such breaches can be especially detrimental in environments that house sensitive data, including personal, financial, or proprietary information.

Furthermore, excessive permissions, even if intentional, pose a significant risk. Every additional permission granted amplifies the potential attack surface for malicious entities. Adhering to the "principle of least privilege" — granting only the permissions necessary to perform a task — is paramount.

Lastly, it's noteworthy to mention the danger of dormant or unused accounts. Often, these are former employees or temporary accounts that were never deactivated. Such accounts, if compromised, provide a direct route for unauthorized access.

In conclusion, while AWS offers robust tools and features to enhance business capabilities in the cloud, ensuring the proper configuration and management of IAM is indispensable. Organizations need to be diligent in their AWS IAM practices to avert possible threats and safeguard their digital resources.