4/19/2018 Twin Cities chapter meeting
Presenting on "Are you prepared to go to the cloud?"

Office 365 and authentication.
People using internal AD servers.
Comments about not synchrizing to the cloud because of concerns with your identities being on Azure (public, phishing). Larger organizations don't have that option, they have to auth to Azure.
The movement to 2nd factor.
Address the concerns with where your credentials are at on Office 365 (the cloud).

Directory services pieces with Azure. What is the synchronization? ADFS and AD Connect. Licensing issues.

OneDrive. People have the ability to download to a home PC. Policy in AD can prevent this.

He brought up SecureScore.

Enterprise Mobility and Security from Microsoft.

A client chose to use ADFS because they didn't want to leave any auth in the cloud, but they already have multiple data centers in diverse locations.

Cost and complexity of rolling out cloud.
Mayor of Burnsville. Public incident.

IP whitelisting.
We whitelist our IP space so that only it can access our cloud instance. Does O365 have that option.

Data governance and classification.

Reporting and monitoring of the data that you have governance around. How do you govern things like email and office docs?

OMS -> Baked into Azure called Log Analytics

Backup and recovery. Ransomware.

Keeping up with changes. Microsoft is constantly changing products.

What do you do when you fragment with your on-prem security tools? "A way to break defense in depth."

VDI instance. Protecting data from moving.

Shared responsibility model.

Risk transference.

Shadow IT, and things that are already on the cloud outside of the well planned cloud migration.