**Minutes for the Fall 2018 Cybersecurity Club Meeting**

**November 7th, 2018 at 5:30 PM in Stright 107A**

**Presenters:** James Lutz

1. James began his presentation on full disk encryption.
2. James introduced encryption and explained what it is.
3. What encryption is not. It does not protect against malware. Full disk encryption only protects your data on a hard drive before it is booted to.
4. Partitions are encrypted by block and encryption info is stored in the header.
5. Encryption key is encrypted with a protector. Protectors can be a password, key file on a USB, a smart card, and more.
6. BitLocker is a popular full disk encryption tool that comes with Windows.
7. VeraCrypt is another popular tool used for Mac and Linux. VeraCrypt doesn’t have anything indicating encryption in the header.
8. dm-crypt is a disk encryption tool for Linux.
9. Mac also has FileVault.
10. Self-encrypting drives do everything themselves. All encryption and decryption is done on the drive itself. These have been used in the industry for a while.

The meeting concluded at 6:03 PM.