Encryption

To ensure data is not being compromised we strongly recommend, and in some cases require, drives to be encrypted

See Chemistry IT project:

- Encryption project for Chemistry and Physics

See also

- http://arstechnica.com/gadgets/2015/08/phone-and-laptop-encryption-guide-protect-your-stuff-and-yourself/
- https://www.facebook.com/GoogleTakeAction/videos/vb.924932914232399/939211039471253/ (Google promoting encryption, 9/2015)

Mac Encryption

Windows Encryption

Disk-level and file-level encryption is somewhat supported at Cornell (and some in ChemIT have some familiarity with it)

To-do: Current offering is not as solid as emerging options appear to be for Windows. Once emerging options are solidifies operationally and support-wise, get CIT's:

- Documentation.
- Recommendation(s).
- Central key-escrow details and process.
- Clarify central support and expectations for either technical staff and end-users.

ChemIT's current capabilities

- Consultation regarding encryption
  - Risk management, whether encryption or its alternatives, is as much an issue of ones behaviors and attitudes as it is about technology.
  - Note: We personally have very limited experience with encryption.
- Benefits of encryption.
  - Use-cases when it's helpful. And when it's not helpful.
  - Encryption can represent unnecessary bother and risks in meeting some needs.
- Alternatives to encryption.
  - If the data is not on your laptop (for example), there is no need to have encrypted data on the laptop.
  - Identifying benefits and risks of various alternatives.
- Risks if using encryption. Currently, must self-escrow keys.
  - You may lose your data because of the encryption, through technical failures or losing keys.
  - Your backups may not be set up correctly relative to your encryption choices.
  - There is no university support for failed situations, including from ChemIT staff.
- Very limited training via some show-and-tell related to encryption or alternatives.
  - We cannot provide on-going support for anyone choosing to use encryption.

Future direction

If and when Cornell provides central support for file-level or disk-level encryption, ChemIT can naturally expand its services as appropriate.

- Coming as part of CU's MS Configuration Management service

Continue to gauge demand within CCB. Requests for the service are almost non-existant so far. We recognize that although CCB use-cases seem low, but perhaps some risks are well hidden. (Faculty do travel. What data do they take with them?)

- Would those same, well-hidden use-cases avail themselves of an encryption service?

Possible, if deemed sufficiently valuable to CCB:

- Advocate for a central encryption service.
- Set up a service.

- R&D, then testing promising solutions. Vetting can take a lot of time to uncover all the undocumented "gotchas". Develop recommendations, along with recommended alternatives.
- Invest in, and bear the risks, associated with provisioning a local key escrow.
- Invest in documentation and maintaining that documentation.
- Provide in-person support for when things are going well. And for when things do not go well, when a higher technical competence is expected, often specialized.