Digital Security

Threat modelling and prioritizing

What assets are we trying to protect? / What would consequences of not protecting them to be?
- Sensitive data
  - Member info
  - Financial info
  - Operational data
  - Website, social media accounts
- Strategy documents and discussions
- Action planning
- Embarrassing/problematic communication

Who are we trying to protect them from?
- What resources do they have?

Consider legal discovery as well was surveillance/hacking

End product: Prioritized hierarchy of assets, threats, strategies

Securing (static) data

Securing devices
- Laptops
  - Full disk encryption with strong passwords and secure back up of those passwords
  - Depending on threat model, enable "Where's My Mac" feature on Macs
  - Keep them with you! Don't leave in cars, on coffee shop tables, etc.
- Phones
  - Strong passphrase
  - Depending on threat model, enable "Find My iPhone" on iPhones (is there an equivalent for Android?)
  - Consider how to manage Google Suite and other document sharing on phones

Solid, encrypted back up
- Test restore
- Monitor whether all computers are being backed up
- Protect old versions from most users in case current data is wiped
- Compliance with data retention policy

Data retention policy
- We have policy, need compliance plan

Online accounts
- Use two factor authentication
- Evaluate Box security and other options (see collaboration tools below)

Securing communication and dynamic data

Email optionsl
- Stick w/ Gmail
  - Use Two Factor Authentication
- Move to Proton Mail
  - Would increase security of internal email, doesn't impact external mail
- Use PGP Encryption
  - For high stakes external emails
  - Use Mailvelope with Gmail
  - Requires significant technical ability to use properly, false sense of security if you don't

Messaging
- Use Signal for texting
  - Installing on chrome makes it easier

Collaboration tools
- Secure file sharing
  - share.riseup.net
    - For quick sharing of normal size sensitive files
  - onionshare
    - For secure sharing of large files
  - evaluate Box security
  - consider whether our threat map requires a more secure solution
    - Sandstorm.io
    - OwnCloud
- Team chat and project management
  - Crabgrass
  - Sandstorm.io

Action plan

Do easy, high impact things immediately.
- Two factor authentication on Google, Dropbox, FB, Twitter, Etc
- Have everyone install and start using Signal for all messaging and sensitive phone calls
- Turn on full disk encryption on all computers, enforce strong passwords
- Use a password manager for org passwords, and upgrade all passwords

Develop doc and email retention policies and practices
- What should never be generated in the first place
  - Train and enforce on acceptable communication
- What gets kept?
- How long is it kept for?
- How is it enforced

Do digital security threat map
- Get outside expert to review?

Evaluate and decide what new tools and practices are needed based on threat map.
- Could include a hierarchical system where highest security/lowest usability is used for only sensitive docs/comms

Don't forget that digital security is only one component of your security/crisis plan