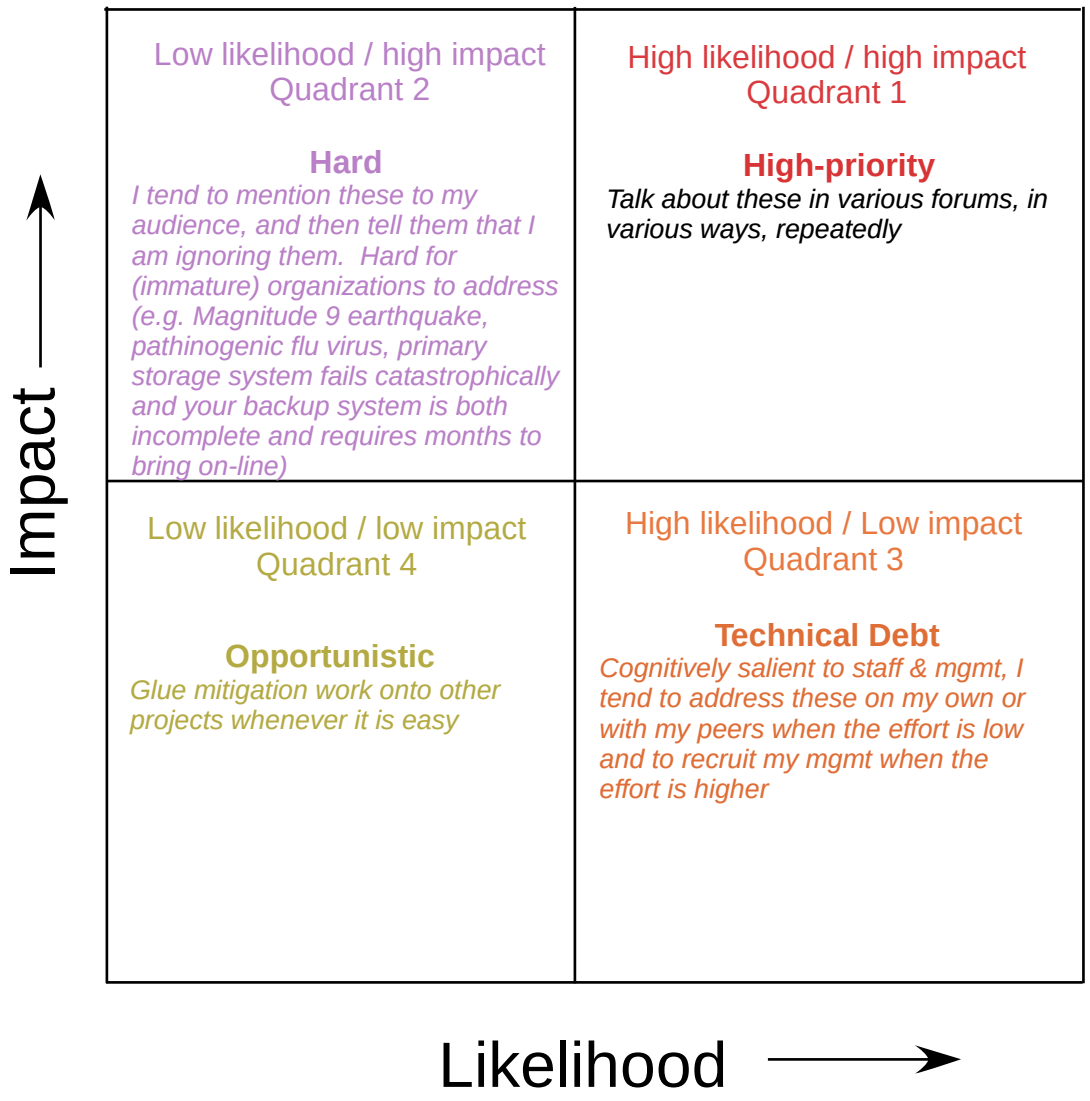
Risk Management Communication Framework



I use this framework to help me guide conversations with peers & mgmt.

Quadrant 1 risks show up regularly in my conversations. Currently, (a) Storage overwhelm, (b) Wannacry, (c) and r Firewall replacement occupy this Quadrant.

Quadrant 2 risks I tend to ignore -- I have yet to work for an organization mature enough to engage on them.

Quadrant 3 risks tend to occupy a lot of my attention -- I admit that they are not necessarily the right place for effort, but they tend to be easier to address: we keep getting pricked by them, so staff & mgmt find it easier to engage the necessary effort.

Quadrant 4 risks I tend to try to ignore or at best glue onto other projects.

This framework tends to obscure Effort, i.e. items which cost a lot to address tend to be ignored, and this framework doesn't handle that dimension well.

Notes

- *Mitigating* a risk is not the same as *Fixing* it -- we may decide to do only a little bit about a risk, just enough to shift its Likelihood or Impact a little farther down the matrix.
- I emphasize conversations -- risk tolerance varies widely amongst people & institutions -- I emphasize talking about risk, as the early part of building the momentum it takes to decide to either *Accept* or *Mitigate*