Business Drivers for Multi-factor Authentication (MFA)

An institution can come to the decision to deploy some form of multi-factor authentication (MFA), or at least an alternate factor, for a variety of reasons. The following illustrates some key business drivers that the MFA Cohortium has identified as reasons to begin deploying MFA within the institution. Each driver is linked with a diagram that illustrates the decision tree one might follow to confirm that the time for an MFA deployment is "now".

Institutional Drivers

Review: Institutional MFA Decision Tree

- Privileged system/server access (e.g. root, network devices)
- Services with higher risk (e.g. sensitive data)
- Combat phishing & other password discovery attacks
- More security for BYOD, mobile access. etc.

User-driven Drivers

Review: User-driven MFA Decision Tree

- MFA as a personal choice
- Users are concerned about their personal data
- Users are concerned about their passwords being phished/stolen/discovered
- Demonstrate potential & usability of MFA

Achieve Assurance Level Drivers

Review: Achieve Assurance Level MFA Decision Tree

- Certification for InCommon Silver without significant retrofit of password processes
- Establish base for Level 3 or higher assurance
- Alignment with NSTIC goals