|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | **Barrier relevance to technology innovation deployment process** | | | | | | | |
|  |  | Initiation (pre-adoption) | | | | Implementation (post-adoption) | | | |
|  |  | Barrier | Cause | Effect | Source | Barrier | Cause | Effect | Source |
| **Owner of deployment barrier** | Individual | Many decision makers are risk-averse | * Their job is pegged to how the company does financially (PV1\_DI, Pos. 28) * They do not want to bear the consequences if the innovation does not pan out (PV1\_DI, Pos. 28) | * They stick to the status quo and are innovation averse (PV1\_DI, Pos. 28) * These innovations lose out in the prioritization process (PY2\_DI, Pos. 26) [see Pr\_TechPerf] | PV1\_DI, Pos. 28  PY2\_DI, Pos. 26 |  |  |  |  |
| Need to fight for executive mindshare around innovations | Executives are focused on keeping the doors open and making it another quarter | Not all innovations can simply be adopted | PY2\_DI, Pos. 4 |  |  |  |  |
|  |  |  |  |  |  |  |  |
| Organization |  |  |  | CS1\_DI, Pos. 22 | Manufacturers want a phased approach and not grind the conventional processes to a halt at once | Cold start problem: No one wants to be the first adopting the technology [see Pr\_SocialInf] | They are slow at rolling out new technology and reticent to be clear in their communication about the change in process | ETC1\_DI, Pos. 50 |
| Providers operate on very thin margins (1%-2%)  “Roughly 20 years ago, the average industry in America would spend about 7%-8% of its revenue on IT. So, consumer companies, others, banks would spend like 12% of their revenue on it because managing all their data was so critical. The average hospital in those days, this is going back again 20 years ago, was spending like 2%-3% [quote].” |  | Have little capital available to invest in new innovation (20 years ago 2%-3% vs. the average industry in America spends 7%-8% of its revenue) | CS2\_A2\_DI, Pos. 8 | System openness:   * Health IT vendors keep their systems as closed as possible (CS2\_A2\_DI, Pos. 26) * Are afraid that if they open up their systems for others to plug in this will lead to data breaches and security issues (CS2\_A2\_DI, Pos. 26) * Health IT vendors are afraid of data privacy and security threats concerning patient data, as well as the implications on their brand and their integrity (PV1\_DI, Pos. 4) | Are afraid that if they open up their systems for others to plug in this will lead to data breaches and security issues (CS2\_A2\_DI, Pos. 26) [see Pr\_RiskTrust] | Health IT vendors keep their systems as closed as possible (PV1\_DI, Pos. 4) | CS2\_A2\_DI, Pos. 26  PV1\_DI, Pos. 4 |