# Assessing Risks

There are always risks associated with using any kind of technology. The challenge is to discern whether the reward outweighs the risk. As CU's move toward providing more services from outside sources, this risk/reward conundrum becomes even more important to examine.

So how do you go about assessing risk and determining if the rewards are worth the risk? The first step in any risk assessment is determining the potential areas that security could be compromised. Particularly, if you're working with a new technology or vendor, you may want to consider talking to someone who already uses the technology or vendor and see what they've learned about the potential security holes.

The next question to ask is, "how do I plug the holes or what does it cost to plug the holes?". If it costs a lot to plug a hole does that kill the project? Not necessarily. You may decide that the reward is great enough that the level of risk is acceptable. You've identified and documented the risk and that helps you to measure the rewards against the risk.

While looking for risk you will want to think about the following:

1) What is your organization's level of risk tolerance? Some organizations are much more risk-averse than others.

2) Does your CU routinely explore new ideas and processes? There is always some risk in doing new things, but if you do this often, your organization is probably more attuned to risk evaluation and done the kinds of things that generally mitigate risk.

3) How easy it to get the data? If it's easily recreated, then it may be less valuable than data that takes lot of resources to create. Doing regular backups and creating mirrored databases help to mitigate this kind of risk and contribute to your overall disaster recovery capabilities.

4) How critical is the data? If the data is incidental to the operation of the CU, you may not care too much if it's lost. However if it's a part of your mission-critical systems, you'll probably care a lot more.

5) Can the risk be mitigated, if not eliminated? You might be able to cost-effectively reduce the risk to a point that the remaining risk is acceptable.

Let's take a look at an analysis of a product you may be looking at today, account aggregation.

In the case of Aggregation, the reward is the ability to look at your current financial picture without the hassle of jumping around to a dozen places to gather the data and write it down. There are 2 levels of risk involved. First, someone will be able to access and look at a member's finances because they've somehow acquired their aggregation account number and password. They won't be able to do much other than look because today most aggregation sites are only gatherers of data. Down the road this may become more worrisome when the aggregators begin to have transactional capability. Then the issue of liability really looms large. There are a number of regulatory bodies that are looking into that issue and we have to trust that they will come up with a reasonable solution to that dilemma.

The second level of risk is that the aggregator's account number/Password/PIN database is compromised and someone is able to access each of your member's individual accounts. This is more serious because, assuming that the FI has a function that allows transfer of funds to someplace else, potentially someone could clean out an account. In many cases these kind of external transfers are limited to already established relationships or take some time to set up. Typically someone would want to get the money and get out quick to lessen their risk of being detected, so taking time to set up an external transfer is not necessarily something they would like to do. Given that, what could a hacker do to you? They could look around at your accounts and balances, maybe transfer some money to one of your other accounts at the same institution, but not really anything that is harmful (maybe a little unsettling).

So with that as background, what are the aggregators doing to mitigate the risks. The first level of risk is no more risky than accessing your regular home banking system. You should remind member to protect their account number and password no matter what system they're using.

# Assessing Risks

Based on the current state of aggregation site security, the second level of risk is terribly small. Most of these companies use computer systems that have security that equals that of the best in the world. Starting at the operating system (OS) level. The OS will have been certified against attack at least to the C2 level (The federal government defines C2 as secure and B2 as trusted). On top of that security is encryption for the data (account number/PIN) that is stored. On top of that is encrypted access to the encrypted data using a different encryption algorithm. On top of that is the account number and name for access to the encrypted information. This kind of layering, makes it extremely difficult for someone to attack a system and retrieve the aggregated account number and PIN. And as discussed above, if they do get in, then they have to go through some additional work to make it pay off.

There is very little you can do where there is no risk and just living is risky (did you read about the 200 lb refueling nozzle from an airplane that fell through the ceiling of a house?). Only you can decide whether the reward is worth the risk by doing your risk assessment homework before committing your institution to a new product or service for your members.