Core system relationships key as tech evolves

Robert Neville is president of Modern Banking Systems Inc., Ralston, Neb. MBS has been providing technology solutions for more than 50 years and specializes in core banking systems, among other services. Neville spoke with NorthWestern Financial Review about current and future issues surrounding core banking technology.

NorthWestern Financial Review: What are some of the things that differentiate core providers in 2017?

Robert Neville: Service is definitely an issue front and center out in the marketplace today. As providers get bigger, client institutions tend to perceive, real or otherwise, that service takes a hit and becomes less personal. Size is also a differentiator. There are the big four and the rest of us. There are certainly pros and cons to doing business with both to be considered, much like banking with a community bank versus a mega bank.

NFR: How does core technology scale up for banks on a growth trend or considering a merger?

RN: Typically in-house institutions have a fixed “upfront cost” on their core system with built in growth capacity at minimal additional cost. Outsourcing-institution costs typically are based on asset or licensing (users on the system) volume and costs escalate quicker with growth or mergers. It’s also very important to consider de-conversion/conversion costs in the equation and get those in writing ahead of time.

NFR: What are some of the most pressing issues banks face on the back end to satisfy regulatory requirements and how is tech addressing those challenges?

RN: We are in the midst of Same Day ACH. In-house banks are affected most in the back room because it can cause additional labor costs as they move end-of-day update processing later to comply. I’ve seen a greater interest in moving to outsourcing as a solution in this area. TRID is another concern as the CFPB will be requiring financial institutions to report up to 48 new data fields per borrower. At MBS, we’ve added a host of new user definable data fields and I’m sure other vendors are moving in the same direction.

NFR: On the security front, where do you see banks being the most vulnerable and what sort of solutions are available to plug the holes?

RN: Cyber security worries probably keep most bankers awake at night. Ransomware, phishing, email scams, etc., are all on the rise. Banks need to review their backup systems and policies to be sure they have good clean data to go back to if they have an event that is caught early. In addition, adhere to industry best practices on replacing firewalls at least every three years, stay atop patching systems, keep anti-virus up to date and continually train your staff to hopefully prevent or limit risks.

NFR: Any thoughts on the ever-growing reliance on cloud services when it comes to banks?

RN: There is still a fair amount of skepticism of the cloud, at least in the community bank space. Do your due diligence; know where your data is physically being stored, with whom, and what controls and data security systems are in place. And then, where are those systems backed up to for disaster recovery purposes. Strong due diligence is key here to relieve concerns and limit risk.

NFR: What sort of tech do banks not employ now that might be common place down the road?

RN: Fintech is definitely a laboratory for financial innovation in the industry. The OCC has recently opened an Office of Innovation to address “responsible innovation.” You could see technology like “behavioral biometric security,” advanced controls on credit/debit cards controlled by the consumer to affect/limit behaviors of the card holder, or artificial intelligence using heavy data analytics to affect desired outcomes in product and service goals.

NFR: Contracting with core providers has been a challenge for some community banks. What’s your approach to this and what should a bank keep in mind when finding the right partner?

RN: For years banks and vendors have built trusted relationships. That’s a good thing. Over time, client institution needs grew, and products and services were developed by vendors to address those needs. This resulted in additional contracts or master agreement addendums that had terms to finance those additions that did not match original contract start and stop dates but were executed without much attention. Now there is a push to “co-term” all agreements to put the client in a better position to make a clean change of vendors or target a date of a bank sale to prevent costly surprises. To help clients achieve this, the vendor and client can either choose to shorten or lengthen mismatched contracts on each end. Vendors need the opportunity to recoup their costs with a profit while client institutions need to better position themselves satisfying their objectives. Bottom line, both parties need to thoroughly review contracts with each other to understand the ramifications. Vendor management is bringing this to the forefront.