Introduction

When it comes to information technology, speed, agility, and reliability are paramount, and generally go hand-in-hand with increased performance and productivity. But, in the financial services industry, the formula is a little bit different. Yes, speed, agility, and reliability are key to boosting performance and productivity, but banks and other financial institutions must also operate within the context of very strict security and privacy concerns — not to mention regulatory mandates. Striking a balance between agility and security can be very challenging — especially for small and mid-size institutions, and especially in an age when users willingly engage in potentially risky online behavior because the rewards are greater than the perceived risks.

Indeed, the underlying technology behind mobile, cloud computing, and social media have combined to challenge the resources of IT departments at banks — and their legacy infrastructures—to their very core. To be agile, banks need to deploy technology that supports their innovative products and services that differentiate, create customer loyalty and increase business growth. This requires banks to build secure platforms to support new technology such as mobile and social. But their legacy infrastructure is generally not up to these tasks, so upgrades or new capital expenditures are required. The trouble is, even if a bank has the money and in-house skills to upgrade legacy infrastructure to securely meet today’s needs, those needs are very likely to change quickly as new technologies and client demands emerge.

Investing in capital-intensive IT, then maintaining and supporting that infrastructure and the facilities required to house it, often puts banks at a competitive disadvantage. It siphons off discretionary funds that would be better spent on developing new products and services to remain competitive. IT consumes significant capital and operating overhead. In fact, after human resources costs, IT is the largest line item expense for banks, says Roji Oommen, Managing Director of Financial Services at CenturyLink, a managed services and network provider. “Today, some 80 percent of the bank’s IT budget is used for the care and maintenance of the current IT infrastructure, leaving only a small amount for improving the customer experience through technology,” Oommen explains.

Challenge

Banks today are facing increased competition, a demand for services across a variety of digital platforms, and increasingly complex security and regulatory requirements.

At Stake

Banks that cannot exceed consumers’ expectations will lose existing and potential new customers to their competition.

Solution

Banks—especially small and midsize banks—can reduce costs and achieve ongoing agility by partnering with an infrastructure-as-a-service provider that can offer rigorous operational and security controls, scalable and highly available IT infrastructure, and expertise.
So, what’s a bank — especially a smaller bank, with relatively constrained resources available — to do? The answer is certainly not “nothing.” The IT world has changed, and the historic approach of investing heavily in corporate data centers as part of a 10-year IT plan no longer is viable. Technology is changing too fast, and customers are more demanding than ever.

Changing Security Landscape

One of the biggest challenges for banks today is security. The landscape is changing, with sophisticated new threats and players adding to the complexity seemingly every day. “Online banking has become a prime target for cyber criminals and nation states trying to steal confidential information,” Oommen says.

Keeping up can seem overwhelming, but banks that don’t risk losing, well, everything. Just one breach is often all it takes for consumers to take their business elsewhere, and the damage to a bank’s reputation is often irreparable.

To protect customer data and meet or exceed regulatory requirements, there are several steps banks can take:

1. **Provide security in depth:** Not all data in the bank requires the same level of security. Marketing and generally available bank information, for example, requires far fewer security precautions than customer account and personal information. Layered security for each level of data can help contain IT costs.

2. **Don’t skimp when it comes to security expertise:** It’s important to work with an experienced managed security provider that can prevent, detect and respond appropriately to a potential breach. Bear in mind that good people come at a high cost, and require ongoing training and certifications to maintain the requisite skills.

3. **Know the biggest threats are those unseen:** Small and mid-size banks that run their own data centers may only be aware of potential attacks within their facility. Bank IT personnel should tap into all of the major security agencies to stay up on news, as well as tap into the banking industry’s online community. This is a full-time endeavor, requiring resources and expertise, often taking less of a priority than other projects if managed in-house.

4. **Position the IT department to be able to turn on a dime when regulatory and security requirements that affect your location and industry change:** Regulators look for clearly defined and documented policies and procedures that address ongoing regulatory and security requirements. Be sure your institution is ready.

Easy, right? Unfortunately, no.

The trouble with these best practices is that they are out of reach for many financial institutions, especially small and mid-size banks that don’t have the budget or the manpower required to make it all happen. Rather, today’s retail banks are in a period of transformation, particularly regional banks that must meet the same stringent regulatory requirements as top tier banks but rarely have the technical in-house expertise or the deep pockets to compete.

“Today, some 80 percent of the bank’s IT budget is used for the care and maintenance of the current IT infrastructure, leaving only a small amount for improving the customer experience through technology.”

**Roji Oommen**  Managing Director, Financial Services, CenturyLink
Rather than building a monolithic data center that requires specially trained engineers and massive investments in support and services, today’s successful mid-size, regional and community banks may consider a hybrid IT approach — a combination of services including colocation, cloud and managed services to scale and continue to meet future requirements. Transferring some of the burden to a managed service provider enables financial institutions to channel their energy into developing applications, products and services that will help build brands and increase revenue — rather than just closing existing security holes and girding for security threats that haven’t made themselves known yet.

Compliance Concerns

Of course, when it comes to financial institutions, government regulations and compliance are very serious business. It can be difficult for banks to meet regulatory demands — a challenge exacerbated as banks try to achieve compliance using out-dated systems and as regulations shift and grow more complex.

“Bank regulations change often,” says CenturyLink’s Oommen, “and how regulators interpret privacy and security changes over time.”

All U.S. banks, regardless of size, are required by the Federal Deposit Insurance Corporation Improvement Act of 1991 to maintain a percentage of overall capital in liquid assets based on size and the types of investments made. The purpose of this act was to reduce the number of bank failures by ensuring banks have sufficient assets; it also means that for smaller banks to meet this requirement, they will have fewer assets available for IT investment than their larger counterparts. More recently, banks have had to meet new liquidity standards set by the Basel Committee in response to this decade’s severe economic crisis.

In addition to the mandates addressing asset liquidity, regulators also have rules about data privacy, security and the ability of customers to access their accounts — taller and taller orders these days given the 24/7 nature of computing and the number of platforms and devices customers are using.

The bottom line is that it typically costs banks more to keep up with all of these changes than it would to partner with an Infrastructure-as-a-Service provider. “Even smaller banks can compete as peers with larger banks that have significantly larger budgets,” says Oommen.

“Even smaller banks can compete as peers with larger banks that have significantly larger budgets.”

Roji Oommen  Managing Director, Financial Services, CenturyLink

Today’s Retail Customer

According to Ovum Research, IT spending for online banking will increase considerably by 2018 (6.4 percent growth in 2014, reaching $10 billion by 2018), with other channels, such as mobile, growing even faster. This is mainly because the functionality of digital channels is maturing and customers are increasingly able to use them, the firm says.
Today’s retail banking customer is less likely to walk into a branch to conduct a transaction. According to the Consumers and Mobile Financials Services 2014 report from the Federal Reserve, 87 percent of the U.S. adult population has a mobile phone, and 61 percent of those devices are smartphones. More than half of all smartphone owners used mobile banking applications in the past 12 months, and another 12 percent anticipate doing so in the next year. And that’s just mobile banking, which the Federal Reserve defines as access to the bank from a smart phone. The same report says some 72 percent of respondents have used some sort of online banking, from a mobile device, tablet or PC in the past year.

Indeed, customers are depending more and more on their mobile devices to conduct bank transactions and track their accounts. And retail customers expect that their information will be secure. Here again, banks have a choice: They can invest heavily in a data center designed to meet the current data security profile of defending against breaches, or they can choose to utilize an outside partner that has the professional staffing and financial resources to address emerging threats.

Banking regulators acknowledge that customers sometimes engage in risky behaviors with their phones and mobile devices, such as checking account information over an insecure wireless network or using weak passwords. “Many banking customers today do not utilize the traditional passbook or check registers to keep track of their bank balance,” adds Tony Kroell, Senior Director of Industry Marketing at CenturyLink. “Banks have to deliver balances to remote locations instantly.”

Ultimately, says CenturyLink’s Oommen, it is the bank’s responsibility to ensure the customer transactions are safe and secure: “It’s the bank’s job to protect its customers.”

But even with some of the nation’s largest banks investing millions of dollars in hardware and software to improve the banking experience for their customers, smaller banks can compete. The key, says Kroell, is to leverage an Infrastructure-as-a-Service provider that can put the regional or community bank on the same playing field as the larger banks.

### Experience

But while incorporating the expertise of an Infrastructure-as-a-Service provider can give regional and smaller banks the ability to compete with larger financial institutions, picking the right provider is crucial. There is no one-size-fits-all, nor is there one approach that fits all. So how can you determine if a services provider is right for you?

In addition, whenever possible the potential customer should tour the Infrastructure-as-a-Service provider’s physical site. Here are some items to look for that can tilt the balance between selecting and rejecting a provider:

1. Does the provider maintain appropriate physical security?
2. Are servers physically caged with additional security measures employed to control access?
3. Does the provider employ appropriate access management physical security barriers to keep potential staff or visitors away from secure areas of the facility?
4. Does each employee have to scan a badge or otherwise show identification individually, or can multiple employees enter secure areas without providing ID?

### Migrating to an Infrastructure-as-a-Service Environment

#### Components

- Technology
- Risk and Compliance
- Information Security
- Operations
- Sales & Marketing
- Human Resources
- Legal

#### What Operations to Outsource

- Repetitive and non-strategic operations
- File & Print, Email, Backup and other operational functions
- Basic storage requirements
- Database management
10 Issues to Ask Before Signing On the Dotted Line

1. Do you have experience with financial institutions of a similar size as yours?
2. Do you have knowledge and expertise with relevant government regulations and compliance requirements?
3. Can you provide copies of audits and compliance documents that demonstrate that your facility is secure and meets its own compliance requirements?
4. How can you help us compete effectively with other banks while reducing our capital expenditures and long-term fixed costs?
5. Can you provide information about your staff and how our account will be managed? Will we have a single point of contact in case of emergency? Do your policies and procedures match those of our company? Is your corporate culture similar to ours?
6. What is your own disaster recovery plan, and how would you handle an emergency that could impact the bank?
7. How quickly can you spin up or down additional servers if we want to test, say, new marketing campaigns?
8. What if we decide to switch providers? Would there be any repercussions? Fees? What would happen to our data?
9. How would you scale to meet our future needs, including support for disparate hardware and software?
10. Can you describe your own security plans and supply chain? Where will our data be stored? Who will have access to it? If the provider cannot guarantee your data will be secure and meet all of your security mandates and needs, stop right there. This is not the right partner for you.

Conclusion

A successful engagement with an Infrastructure-as-a-Service provider will allow the bank to concentrate on enhancing its product offerings and customer service. From an operational expenditures standpoint, the bank will not only reduce its capital expenditures, but will also see reduced power consumption for systems and HVAC; as well as a potential reduction of real estate costs, insurance expense, and facilities management expenses.

Banks that follow the approach outlined in this paper will be well-positioned to increase revenues and focus more on the core business of banking while shifting data center business expenses to a professional service provider. These capital cost savings combined with the ability to provide greater customer satisfaction and generate new revenues will sustain and propel the bank as it takes advantage of the Infrastructure-as-a-Service that is transforming the financial services industry.
Qualities to Look for in an Infrastructure-as-a-Service Service Provider

- Proven experience supporting banks of a similar size
- Maintains appropriate and current compliance certifications
- Ability to meet the compliance and the data, physical and personnel security requirements of the bank
- Demonstrated expertise in Identity and Access Management, Encryption, Authentication, and other essential data security practices
- Maintains a staff of qualified service and support engineers to meet the bank's needs
- Can support the bank's existing and future IT infrastructure requirements, including incorporating the data center needs of potential mergers and acquisitions
- Copies of security audits and written policies and procedures for review by bank
- Does the provider have a corporate culture and business philosophy that matches the bank's culture and philosophy?
- Will the provider be a trusted advisor and partner or merely a commodity services provider?

Questions each key stakeholder should address before selecting a service provider

CIO

- We are a Tier 2/3 bank with approximately 50 branches. How will my physical network change? Will I be able to reduce my IT footprint and if so, what impact will that have on my budget requirements?
- What kinds of staffing changes will I need? Will the expertise of my staff need to change if I outsource vs. in-source?
- My bank currently is not using virtualization. What will I need to know about virtualization if I decide to outsource? What happens to my legacy applications?
- How will my server and storage requirements change?
- How do I qualify a potential service provider? What do I need to know about the provider’s technology expertise to ensure that my existing applications will run correctly in the hosted environment?
- Does my proposed service provider have a pedigree in supporting banks and financial institutions? Do they understand our industry’s specific drivers and requirements?

CISO

- What questions should I ask my service provider about their own security policies and procedures?
- What policies and procedures does the service provider have in place, including the prescreening of its own staff, to ensure that my customers’ data is safe and secure?
- How will my risk profile change if I outsource? What assurances can I get from my provider that will improve my risk profile?
- What auditing and security tools do I need to ensure that my network remains safe after outsourcing? What levels of auditing and testing will the provider allow me to do against their network?
- What security credentials and industry memberships does my proposed service provider bring to the table?
About Hybrid Infrastructure Solutions from CenturyLink Business

CenturyLink’s Hybrid Infrastructure solutions infuse agility into IT infrastructure, whether your business is challenged with controlling costs, managing performance, or scaling and expanding into new markets. CenturyLink is recognized as the No. 2 retail colocation provider, with an extensive global footprint that includes more than 55 state-of-the-art data centers across North America, Europe, and Asia, with over 2 million square feet of raised floor space.

About CenturyLink Business

CenturyLink, Inc. is the third largest telecommunications company in the United States. Headquartered in Monroe, LA, CenturyLink is an S&P 500 company and is included among the Fortune 500 list of America’s largest corporations. CenturyLink Business delivers innovative private and public networking and managed services for global businesses on virtual, dedicated and colocation platforms. It is a global leader in data and voice networks, cloud infrastructure and hosted IT solutions for enterprise business customers.

For more information visit www.centurylink.com/enterprise.

CFO

- What is the impact on the bank if we move to an OpEx model instead of a CapEx model?
- What level of compliance does the service provider have and what audits has it passed?
- Every service provider promises savings? Where can I actually expect to see real savings and where am I just transferring expenditures from one provider to another?
- What is the service provider’s experience in serving banks like mine?

- How will the service provider help us combine computer operations in the event of a merger or acquisition?
- Has the service provider faced any enforcement actions from the Federal Financial Institutions Examination Council (FFIEC) agencies, including the Federal Reserve System, FDIC, or Comptroller of the Currency, or Consumer Financial Protection Bureau?