

## Cottage, Please? How ISOs Are Answering Requests for Remote Access

Is work something you do, or is it a place you travel to?

Telecommuting, often considered a “return to the cottage industry,”<sup>1</sup> started in the early 1970s, linking offices with some 1,200 band modems and telephone lines. By the early 1980s, branches and home workers were able to connect to company mainframes from their personal computers.

As networking technology improved, a decrease in cost and an increase in performance continued the cottage industry revival. This phenomenon is gaining momentum. Bank managers connect to the bank’s network when they go on the road ... and even when they stay home sick.

For the most part, however, banks are not early adapters. “We currently do not allow users to have remote access,” reports Cindy Krumanaker, vice president of information systems for First Federal Savings Bank, Huntington. “Though the subject has come up, we simply do not see the business case outweighing the risks.”

“So far there are only two of us who have access,” says J. Craig Buse, vice president IT manager of Springs Valley Bank and Trust Company, French Lick, “and we’re both in the IT department, so it’s easy to control.” That’s two out of 80 employees.

Some banks are slowly dipping their toes into the water. “As a general rule, we do not allow people to work from home,” states Doug Bell, systems and vendor manager for Indiana Bank and Trust Company, Columbus. “There are a few exceptions. We do allow those with a demonstrated need to access e-mail remotely with Outlook Web Access. We provide smart phones to some people to allow them similar access to e-mail and calendar functions. Our network engineers can access the network via secure VPN2 from home using bank-owned equipment to perform work off-site.”

“We allow it only for executive management and myself,” explains T.J. Deckard, assistant vice president and director of IT for United Commerce Bank, Bloomington. That pool of users provides for five people out of 37.

“We’re at about 20 of 1,000 users,” says Dennis Teague, information security officer at MainSource Financial Group, Greensburg. “But we don’t have anybody actually working from home on a regular basis,” he adds. “The number we have authorized is pretty stable now at 20, mostly mortgage loan originators accessing e-mail, the file server and the mortgage origination application. The network administrator and I also have access, of course, with wider privileges for support and monitoring purposes.”

Teague continues, “Don’t forget, most banks already have vendors that are granted remote access for support purposes. We have run criminal background checks on our vendors, as if they were ‘true’ employees of the bank, prior to giving them remote access.”

### Early Adapters

We all see others in unregulated industries link their users to company networks using virtual private networks, deploying thin client access servers (such as Citrix or Window’s Remote Desktop), or even via outsourced services such as Go-To-My-PC and similar technologies. While we watch the price of technology plummet,

## Cottage, Please?

return on investment no longer reigns as an issue blocking the deployment of remote access in banks. The roadblock to the cottage industry revival is risk.

Regardless of how remote access is deployed, there are many caveats to keep in mind during implementation. Though “working from home” has earned its own chat-room acronym (WFH), the process still includes pitfalls and dangers.

As with any technology, benefits must be weighed against cost and risk. Remote access introduces risk not only to the organization, but also to the user.

The early adapters also report cultural issues. Consider employees staying home sick, but not getting better, because they work rather than convalesce. Or workaholics jumping up in the middle of any given night and to log into the office and obsessively check e-mails.

Extended family and friends have to be trained to not drop in regularly. They may assume that people at home in the daytime are not working and have time for unplanned visits.

Children may find it hard to understand why the “office” portion of the house is off limits, or why they need to keep quiet during conference calls. Family pets may not comply with quiet time rules at all.

Deckard of United Commerce Bank adds a twist on the issue of employee risk. “Is it really worth doing this?” he cautions. “There is something to be said about having a clean break between home and work. We have loan officers who already work extended hours and come into the office while they’re on vacation. So we worry about the psychological effects of extending the workplace into the home, and that the increased stress on the employee could introduce additional risk to the bank.”

### **New Adapters**

This author has yet to encounter a bank that allows staff members to work exclusively from home. Instead most banks permit a select few employees to log in from home, and they’re not rushing into it. “It’s been 15 months,” concedes Teague. “If you ask others in the bank, I’m sure they will say they wish we had done it years ago, but I think we’re taking the right approach. By moving in a slow, deliberate process, we’re more confident in the way we’re handling the risk.”

Technology inherently comes with risk, created by threats which can exploit vulnerabilities in order to negatively affect the availability, integrity or confidentiality of assets. The likelihood of a threat’s exploiting a vulnerability, along with the impact of such an exploit, should be measured in order to help the bank prioritize the implementation of controls, which can be used to minimize likelihood and/or impact—and thus risk.

But it’s not simple. Technology throws us curves called “unforeseen vulnerabilities.” Example: We give our children cell phones, then we read about kids getting hit by buses while text-messaging at the bus stop. Because of these curves, we need to go beyond the obvious technology risks (somebody listening in on cell conversations) and consider processes involved with the use of the technology (texting while walking to the bus.) Then we add appropriate controls (forbid texting at the bus stop).

Meanwhile, who is the threat? Is there a hacker smart enough to break VPN encryption? As it turns out, the threat is more likely to be the insider’s boyfriend in large banks, or the inadvertent mistake in the smaller banks.

## Cottage, Please?

“There is enough encryption and enough going on in-between that my biggest concern is the fact that a user could cause a problem, even inadvertently,” admits Chris Bedel, information security officer for The Napoleon State Bank. “The technical risk is the least of my worries. What we will be focusing on is managing the non-technical vulnerabilities through policy and training.”

How do you foresee non-technical risks? The risk assessment needs to look at the assets involved in the remote access process. For example, will remote access users start taking hard-copy reports home or print them at home?

As with any technology process, the controls depend upon the risks, but there is at least one low-hanging fruit: the approval process itself. This control has matured at MainSource Financial Group. “All remote access goes through the information security committee,” explains Teague. “A form is filled out, the committee reviews the form, and access is granted if there is a strong business need.”

“But there has to be a really good reason to give these people remote access,” he continues. “How the requestors answer the question ‘why’ is essential. Snowstorms are not a good reason to grant remote access.”

“We then issue the employee a laptop if they do not already have one, provide training, and make sure they understand the risks. Their access is reviewed on an annual basis.”

It may be harder to shut Pandora’s box than it is to open it. Tearing down the cottage hurts the bank’s reputation and morale, so the approval process must be taken seriously. We are starting to see this problem arise in acquisitions, as acquired bank managers struggle to adapt to the more conservative remote access policy of their new, larger, and more conservative employer.

But no matter how large the institution, it seems to always boil down to the approval process. “Sure, remote access presents a security risk,” says Deckard, “but our threat assessments show the risk to be no greater than that of a small, remote branch office. The temptation to partake in malicious behavior may be slightly higher at home, since the user may feel they’re less likely to get caught, but the controls we have in place to manage risk are equally effective whether they’re downtown, in a remote office, or at home. What it really boils down to is knowing who has the access.”

He continues: “It’s an extension of how access is granted to our system as a whole. If a user is given a level of access in the office that they could not be trusted with at home, should they even have that access in the first place? That doesn’t mean we give remote access to a teller, but our approach does allow us to give remote access as legitimate needs arise and without introducing any significant new risk.”

Teague concurs: “We have mitigating controls, such as background checks and locking down what they have access to. But let’s not fool ourselves. Beyond the same monitoring and detective controls, we have to mitigate malicious data loss for late-at-night workers. The long and short of it is that when approving remote access, we are trusting our folks.”

Technical risks include the classic risks associated with availability, integrity and security. Fortunately most banks are solving this problem by controlling the endpoint.

## Cottage, Please?

Teague suggests that a key to controlling the endpoint is that the bank owns the equipment. “We require approved users to use a bank-owned laptop,” he says. “We have software that verifies they are up-to-date with their AVS and Microsoft patches before letting them on the network. The laptops VPN into the office, and we limit which IP addresses they can hit, which allows restriction by application.” MainSource also requires two-factor authentication on the endpoint.

“We have recently opened the gates a little more to allow loan officers to work offsite,” says Doug Bell. “This is still in a roll-out stage, but the approach is to give them a bank-owned laptop with an encrypted hard disk, and allow them to connect over a VPN via terminal services to front-end loan functions. We could use this model to allow full remote-control connections to desktops in the future.”

The endpoint hosts most of the risk these days, yet some banks can still control the endpoint without owning the equipment. At United Commerce Bank, T.J. Deckard can allow remote access by employee-owned devices. He uses RDC over a VPN connection to log into a terminal server. His firewall can ensure proper practices on the endpoint.

### Future Adapters

Not all banks have rolled out the cottage revival, but more are thinking about it. “We have not allowed remote access to-date,” says Bedel of The Napoleon State Bank, “but we’re thinking about going to it as part of our pandemic planning. Maybe we give critical processing employees temporary, monitored access.”

Bedel admits that the topic is a proverbial can of worms: “We are scrambling with questions like ‘What’s the training required,’ ‘How do we test this,’ ‘How do we secure that,’ ‘Is this plan feasible on our network setup?’”

As with all technology risk management, it works to answer these questions in the following manner:

1. Start with a risk assessment focused on the assets and the process. Think about operational, transactional, security, legal, reputational and compliance risk.
2. Create a high-level, board-approved policy that establishes who approves and revokes access, how often access is reviewed, that training is provided, that employees are required to sign an agreement during that training—all the typical policy requirements. Don’t forget policy staples such as, “No Downloading NPI,” and be sure to integrate this policy with existing acceptable use policy.
3. Create a procedure that focuses not only on the technology, but also on the approval process. Be sure to balance flexibility with the ability to backtrack on decisions (in essence, build do-overs into the procedure).
4. Then choose the technical approach.

Obviously item No. 4 is not as easy as stated. But most banks, unfortunately, start with the technical approach and then, for compliance reasons, back into policy work. Remember that remote access is one technology where a top-down approach will pay.

Think assets. Some banks will confront resource availability. According to Bedel: “A lot of our users don’t have broadband access. We’re in a rural-enough area that it’s just not there, so we’ll need to provide the Internet access as part of our process.”

## Cottage, Please?

The solution: “Our thought is to provide a laptop with a mobile broadband wireless card, using RDC over a VPN to connect to the network. This way we control the Internet connection, which is physically removed from the home network, and we control the endpoint to a degree commensurate with office workstations.”

Now the layers of security can be counted:

1. Hard drive encryption;
2. AVS on the bank-owned laptop;
3. Simplified auditing;
4. VPN;
5. MAC address filtering on the firewall (introducing a second factor of authentication);
6. The network password; then
7. The application password.

The procedure must include training on the laptop’s wireless card and remote access processes, and ensure users have an understanding of what is required of them non-technically to protect the laptop. Beyond that, it should also address expectations.

For example, according to Gary Kern, chief information officer of MutualBank, Muncie, “Having remote access can also give users the impression that systems are available and responsive 24/7, and they aren’t. They run slower during nightly backups, and we typically do maintenance off hours. It’s important to make sure people understand that when you approve their access.”

### To See the Cottage, Adapt to the Understanding

The floodgates are about to burst. While the thought of granting remote access to users who already question security policies is a scary one, the reality must be addressed. To paraphrase Leonardo da Vinci: “To see is to understand.”

In order to properly manage the construction of the modern cottage, commit your fears to paper in the form of a risk assessment. The rest will take care of itself.

<sup>1</sup>“Cottage industry” usually refers to the pre-industrial revolution workforce, would manufacture or mend items from their homes, usually part-time. The system worked in an agrarian society because farmers had free time during winter months to pick up extra income.

<sup>2</sup>Virtual private network

### About the Author: Dan Hadaway, CISA, CISM

*Dan has worked extensively with banks on policy issues, engaging on projects ranging from gap analysis to developing a full policy set for denovo banks. He can tailor his consulting to any size bank, working on simple user-level policies with banks as small as one location to overseeing the entire IT strategy for a publicly held company. He has provided management-level regulatory compliance training for Fortune 500 companies as well as user-level awareness training for the smallest of banks. His strength is helping banks decide where in the "security/compliance spectrum" they should be. He has helped develop risk management programs and processes for banks as large as 2.5 billion and as small as 26 million in assets.*

He is the Managing Partner of **infotex**, an Indiana Bankers Association Preferred Service Provider in several areas, including Information Security Training.