Your Third-Party Risk Outlook

risk management strategic planning

Summary: Third-party relationships are becoming even more important in an increasingly consolidating industry. We offer a few suggestions on how to manage third-party risk.

Microsoft announced people will be able to get bill pay reminders in Outlook and followed up that announcement with another one that indicates you will also be able to pay those bills using email. Apparently, you can just click a button and pay the bill after Outlook scans incoming emails, identifies any bills, schedules payment dates and then pays it at the click of a button. Of course, PCWorld notes that users will have to overcome the fact that we have been told for years by security experts not to click on buttons in email. Still, it is yet another tool to help make our lives easier.

We think this capability could help bankers collect on loans too perhaps. Just structure monthly payments to resemble a bill, let your customer know about it and Outlook might do all the rest. Not bad and it could improve delinquencies even.

In this capacity, bankers might consider Microsoft a key vendor and maybe even a third-party provider. More so than perhaps any other industry, banks must rely on third-party providers to help them efficiently and effectively run their operations. Yet, as community bankers are aware, these vendor relationships come with potential risk too.

As these relationships are becoming even more important in an increasingly consolidating industry, we offer a few suggestions:

Vet vendor systems as you would your own. The weakest link is where you should start, of course, but all vendors need to be vetted and reviewed as if they were an integral part of your internal operations. You might even consider conducting due diligence on areas like HR management and insurance coverage. Regular vendor reviews that coincide with your internal reviews will help you remember to treat them as you would your own.

Don't discount the cloud as an outside entity. Some may forget that cloud services are in fact another third party. They may even be a vendor that holds or has access to some of the bank's precious data. As one online intelligence expert reminds us, "There is no 'cloud'; it's just someone else's computer." In other words, community banks must be careful in the cloud services they use and stay on top of security around these vendors too.

Require third parties to keep their security to your standards. Banks must rely on outside audits of the security operations center [SOC], model validations, other audits, and other information to help ensure that key third-party vendors are up to snuff in the services they offer your bank. If the resources are available, banks should not only review their major third-parties' background checks on employees, but review audit reports where available, as well as details on the vendors' best practices, including facility access. Make sure to have the third party guarantee its security standards and reviews in the service level agreement (SLA), and if possible, the CISO or a security professional at the bank should visit the vendor site as well.

Focus on the potential problem areas first. Given somewhat limited access to the largest third parties, community banks may be forced to pick and choose where to focus their attention. Experts say that first and foremost, it is critical to consider outside parties that have "non-escorted or unsupervised access" to your locations, or have the most unfettered network access to valuable or sensitive data or transactional systems.

LOAN SERVICES FOR COMMUNITY BANKS

PCBB is almost entirely owned by community banks and it does not compete for your business. Contact us to do loan participations as you protect your customer relationships.