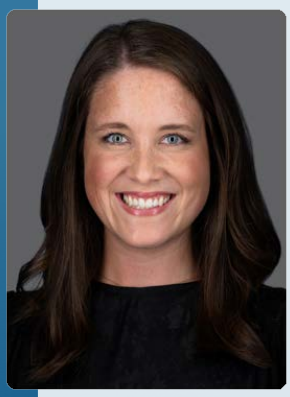
IMAGEQUEST℠

SECURITY DOWN STREAM

VENDOR MANAGEMENT PLAN

Prepare for Examiners' new expectations and protect against new risks with your Vendor Management Plan

How thorough is your bank's vendor management plan? Have you fully vetted your vendors for IT security risks?



By Sammi Jo Shutt
ImageQuest
Security Analyst

From 2020 onward, security researchers have warned of a rise in what's called Supply Chain attacks. These happen when hackers take advantage of vulnerabilities in a vendor's security or secretly install hardware measures that transmit information back to the hackers.

The goal is always to reach the vendors' customers and steal their information.

So far, Supply Chain attacks have involved hackers interested in stealing data for espionage purposes, as appears with the SolarWinds breach. But security experts say other hackers are learning the spying hackers' tricks that successfully kept their

So far, attacks have involved hackers stealing data for espionage purposes, but recent reporting shows smaller community banks without sizeable corporate security measures are a prime target.

malware under the security radar.

It's a scary, dangerous cyber world out there, and unfortunately, requires continuous recalibration to new threats. Going further to assess vendor security measures is one of those recalibrations.

According to a recent article in the American Banking Association Journal, banks are a prime target, significantly smaller community banks without sizeable corporate security measures.

During the pandemic, your bank may have expanded its digital banking measures, inadvertently creating more security risk exposure.

In implementing relatively rapid changes, did your team have time to assess vendors' security risks fully? Did your vendors report on how they assessed their vendors?

The article quotes the ABA's Paul Benda, its SVP for risk and cybersecurity policy, saying no matter what remote banking vendors you used, most of them have their cascade of technology partners working behind the scenes. Bank executives need to know if a third-party vendor has a fourth-party vendor that could create risk for banks "in ways they haven't expected before," Benda said in the article.

The ABA recommends institutions increasingly assess where data is going, who's managing it along the way, and how ***downstream risks may now exist with providers the bank did not even know they were using.***

Thus your traditional due diligence with vendors may need to pick up the pace. Does your banking team have time to repeatedly assess vendors for security risks more frequently than in the past? Or even to dig deeper into the fourth-party vendors your vendors use?

You may think: "They're banking vendors; of course their security is tight!" But remember the Target breach of 2014.

Target had tight security for 2014. But an HVAC vendor accessing its accounts payable portal used only a free, outdated anti-virus program. The HVAC vendor's lax security allowed malware to leap into Target's systems.

And what about the impact of the pandemic? It may have led your bank to adopt more remote banking measures, and it likely also affected your vendors' vendors – some potentially negatively.

Can you be sure all were able to stay up-to-date with security? Or did they hold off on implementing some needed updates?

You need to know the answers. If you don't, it may be time to outsource this work to an experienced IT security vendor, also known as a Managed Security Services Provider, or MSSP.

SO WHAT DOES A VENDOR MANAGEMENT SERVICE DO?

Essentially it assists your bank team with the due diligence of your vendors. It helps you establish a risk rating of your vendor by reviewing how critical the vendors' services are to your overall business and what access that vendor has to your IT systems or Non-Public Information (NPI.)

A well-written and managed vendor management plan can help you determine whether the vendors that access, transmit, store, or dispose of NPI from your organization meet the appropriate regulations and use appropriate security measures. It will also help you answer examiners' questions.

IMAGEQUEST

SO WHAT'S THE FIRST STEP?

To answer the typical questions, you must conduct a risk assessment. Understanding what data you have and where you store it is critical. This includes employee data as well as customer data. Do your vendors have access to either?

Next, you need to understand the regulations that apply to you and your vendors. Do you store or process sensitive data for people that reside in other states? You may need to adhere to specific cybersecurity regulations in those states, such as New York, California, or Virginia.

Consider a couple of real-life vendor examples.

How well does a vendor follow recommended security steps?

Chinese hackers developed a bug that could penetrate on-premise Microsoft Exchange servers, "a type of email server most often used by small and medium-sized businesses," Microsoft said. However, it also noted "larger organizations with on-premises Exchange servers" were affected too.

Microsoft said its initial scan found 400,000 servers at risk on March 1, and by March 11, the company had released "updates covering more than 95% of all versions exposed on the Internet."

Note, the company did not say "remediated." That depends on the server owner and whether they took proper measures.

Sometimes, proper measures mean a complete wipe of a server and re-imaging to eradicate any malware installed. The process can take some time, and if the server is critical to the business mission, the temptation is strong to take a shortcut to get back to work.

A second example:

Do you know how secure your vendors' — and their vendors' — processes are?

Recently, Bloomberg wrote about computer hardware manufacturer Super Micro Computer Inc., based in San Jose, California.

And what about the impact of the pandemic? It may have led your bank to adopt more remote banking measures, and it likely also affected your vendors' vendors – some potentially negatively.

"Many of its motherboards—the clusters of chips and circuitry that run modern electronics—were manufactured in China by contractors, then assembled into servers in the U.S. and elsewhere," Bloomberg reported.

Based on interviews with "more than 50 people from law enforcement, the military, Congress, intelligence agencies and the private sector," Bloomberg found that some Super Micro customers, including Intel and Apple, discovered either malware or extra processor chips in Super Micro equipment. Both the malware and chips sent data back to China.

Super Micro disputed the Bloomberg report, which says the U.S. government investigated the Intel and Apple reports and others but never released information to the public – or Super Micro. Bloomberg said U.S. investigators kept quiet to try to learn all about the Chinese efforts before they disappeared.

In both examples, the cause for concern is not obvious. You need to go beyond the surface to be sure of the vendors' security status when working on vendor management.

SOME OF THE CORE POINTS INVOLVE THE FOLLOWING:

- **What data and systems can your vendors' access?** Is it only electronic data? Is it paper? This exercise will determine how you are going to manage each vendor. Companies that have direct access to your data are going to be scrutinized much more than the company that cleans your office.
- **How are you going to manage these vendors?** Organizations may rely on Master Service Agreements and Non-Disclosure Agreements unless the vendor can provide a SOC report or other certification.
- **What measures do your vendors have in place for business continuity and disaster recovery?** What is their disaster recovery plan?
- **Do your vendors encrypt your data?** Is it encrypted while stored and encrypted when transmitted?
- **And, how do your vendors vet the employees working with your data?**
- **What is the process to initiate and terminate a business relationship when data is involved?** You might move on from a vendor, but how can you be assured that they no longer hold any of your data?

Finally, and most importantly, this must be a written plan with a dedicated plan manager. You cannot place it on a shelf to collect dust. This plan needs to be a living, breathing document for your organization – and reviewed regularly. As the ABA notes, this likely should be more frequent than annually.

What if you encounter a critical business vendor that does not take security as seriously as you do? What if they stall and don't respond to your letter – or claim trade secrets and refuse to supply the information you need?

You cannot assume everyone does what they're supposed to do. In life – and in IT security –some people cut corners.

Then you will have to weigh whether the risk of potential fines – or a breach – is worth continuing with this vendor. You may have to find another.

A vendor management plan can help you avoid unpleasant surprises – such as regulatory fines or a data breach. It's best to make sure your data is safe with vendors who take security and compliance seriously – rather than vulnerable with a vendor who ignores the facts of life with hackers today.