After MoveIT: The Board's Role in Containing a Fourth-Party Breach

By: Emily McCormick, vice president of editorial & research for Bank Director
November 9th, 2023

On May 31, Progress Software Corp. disclosed a security flaw in its MoveIT file transfer tool, a relatively mundane program used by banks and many of their providers. **It wasn't long before some financial institutions and technology companies — including core providers — were disclosing that customer data had been exposed to a group of hackers.** Thousands of organizations and millions of individuals worldwide have fallen victim to the breach, according to the antivirus software firm Emsisoft.

Complicating the situation for a number of financial institutions is the fact that MoveIT wasn't even a third-party service, but instead a fourth party used by a technology solution that was in turn used by banks.

The MoveIT breach occurred almost in tandem with the release of interagency guidance (https://www.bankdirector.com/issues/risk-issues/no-relief-for-small-banks-in-regulators-third-party-risk-management-guidance/) around third-party relationships, which includes regulators' expectations around the disclosures of breaches by bank vendors and the need for ongoing monitoring by banks.

Even for banks that weren't impacted by this latest cyber incident, it offers a real-life exercise for bank boards. And hackers are likely to duplicate this incident, says Ben LeClaire, a principal on the cybersecurity team at the accounting, tax and consulting firm Plante Moran. "I wouldn't be surprised to see [that] we have similar types of attempts and even breaches into 2024, potentially with other types of file service organizations."

Understand the Impact

Data mapping, a proactive process that helps banks understand possible exposures, should provide the first clue in understanding a large breach like the one tied to MoveIT, says LeClaire. **Data mapping establishes where different pieces of information are housed, both within and outside the organization.** If a breach occurs, the bank can then work with the vendor to remediate any issues. Mapping should happen before a breach materializes, during due diligence and monitoring of vendor relationships.

"As data ecosystems are complex and ever-evolving, data mapping provides a foundational element for maintaining data integrity and compliance with various regulatory requirements, as it helps in understanding not just where the data resides but also how it is being processed and protected throughout its lifecycle," LeClaire explains. "It is part of the broader data governance framework and helps ensure that banks are prepared not only to respond to data breaches, but also to prevent them by identifying and securing potential weak points in their data infrastructure."

But it may not have been obvious to some companies that MoveIT, a transfer service, actually held any data, says Allen Eaves Jr., financial crimes sales executive at Jack Henry. "You're looking at a service, or you're looking at a tool that doesn't host data — you're probably not asking a lot of questions about what data they do have and how they protect that data … because that's probably not the key function," he explains. That may require a deeper understanding of how third- and fourth-partner providers' technology works.

Ask Questions About Contracts

LeClaire expects more scrutiny over vendor contracts in the wake of the MoveIT breach.

The FFIEC's IT Examination Handbook (https://ithandbook.ffiec.gov/) puts the onus on banks to understand where the data resides and how it has been secured — including by third and fourth parties. "It's time that we start to put some serious requirements in contractual agreements around the security of the data that these third-party vendors obtain, and then who they would share it with," LeClaire says. "There need to be contractual obligations to make sure that [banks] have the rights to lock down how these third-party organizations are using, sharing [and] sending data." By extension, banks should note in contracts that vendors are performing the same level of due diligence on their own vendors that a financial institution would perform on a third party.

Responsibilities should also be well defined.

Eaves says banks should know, "[W]hat are the risks [if there] should be a breach at that partner? And how is that partner planning on interacting and working with you in the event of a breach?" That's particularly important for critical partners — not just those that are vital to the functions of the bank but also any with access to sensitive data.

Fully understanding those contracts helps banks use them to their advantage. "Sometimes, banks don't avail themselves of their rights under the contract, like ask about the third party's cybersecurity posture or get reporting of data breaches," says John Geiringer, a partner at Barack Ferrazzano Kirschbaum & Nagelberg. Contracts should give banks a path to restitution if the vendor is at fault.

Determine When to Disclose

Banks are required (https://www.bankdirector.com/issues/risk-issues/getting-proactive-about-third-party-cyber-risk/) to notify their primary regulator of a significant cyber incident within 36 hours, and service providers are expected to alert affected banks if such an incident has been detected. The bank may also need to file suspicious activity reports, says Geiringer.

For public banks, the U.S. Securities and Exchange Commission requires the public disclosure of "material cybersecurity incidents" within four days of the bank's determination that the incident was material.

If information has left the bank's network — including its extended network via an exploited fourth party — that bank has been breached, says LeClaire. When a bank has determined via data mapping or other processes that it has been breached, "the requirement to alert [regulators and law enforcement] would absolutely be necessary."

Banks should expect their vendors to be "completely open and transparent" about how they'll work to secure the information, LeClaire adds.

Geiringer advises banks to reach out to regulators and law enforcement as soon as possible, particularly when the bank has been directly attacked. "Many times, law enforcement assistance can help mitigate the event," he says. "For example, international wires can sometimes be clawed back."

Banks should also check their cybersecurity insurance coverage to see if it includes a breach coach to help the bank navigate the event.

Expect More Supervisor Scrutiny

In Bank Director's 2023 Risk Survey (https://www.bankdirector.com/issues/risk-issues/2023-risk-survey-complete-results/) in March, 31% of responding executives and directors reported additional scrutiny of their bank's third-party risk oversight. That promises to heighten on the heels of the MoveIT breach. Boards should stay on top of the issue via high-level cybersecurity overviews from the bank's management team, which should include attacks made against the bank.

Supervisors will pay attention to incident response plans, expecting them to document procedures and testing. **Tabletop exercises could incorporate the MoveIT breach as a real world example to understand how the bank would respond in such an event.** Who would the bank contact? What's the public relations plan? How will stakeholders be notified — law enforcement, regulators, employees and customers? What should the bank expect from the vendor?

Expect to Budget More

"One of the struggles in working with boards in securing their environment is the general understanding of the importance of cybersecurity," says LeClaire. "It's still ultimately categorized as a cost center." Respondents to the 2023 Risk Survey reported a median cybersecurity budget for fiscal year 2023 at $250,000.

When LeClaire conducts IT audits for banks, he often makes recommendations to invest in more advanced monitoring tools that can detect unusual activity or an intrusion in the bank's network. "Fighting fire with fire is one of the necessities here," he says.

And it's important to be proactive. "We are seeing a lag in terms of when an IT department would learn of this sort of event," LeClaire says. "We want the board to be involved up front, so there can be that tone at the top as well as that executive-level oversight of all areas of the business to be able to react to this." Software like MoveIT could be used by various departments within the organization — not just IT. That requires an enterprise-wide view of the risk.

And ultimately, the bank owns the risk — even if a fourth party was the one responsible. "In the eyes of customers," says LeClaire, "it's going to be the bank's fault."

Additional Resources

Third-party risks are further explored in "Getting Proactive About Third-Party Cyber Risk (https://www.bankdirector.com/issues/risk-issues/getting-proactive-about-third-party-cyber-risk/)" and "No Relief for Small Banks in Regulators' Third-Party Risk Management Guidance (https://www.bankdirector.com/issues/risk-issues/no-relief-for-small-banks-in-regulators-third-party-risk-management-guidance/)." FinXTech's Finding Fintechs (https://www.bankdirector.com/issues/technology/finding-fintechs-a-choose-your-own-adventure-guide/) report provides additional information about working with technology providers, including considerations for due diligence.

To better understand changes to the IT examination process, read "The New FDIC InTREx Security Procedures: The Impact on Banks' Digital Strategy." (https://www.bankdirector.com/issues/regulation/the-new-fdic-intrex-security-procedures-the-impact-on-banks-digital-strategy/)

Bank Director's Online Training Series (http://www.ots.bankdirector.com) includes units on cybersecurity, including Ransomware Basics for Boards (https://ots.bankdirector.com/learner/courseinfo/id:238). The cover story in the fourth quarter 2021 issue of *Bank Director* magazine, "Ransomware Attacks Heat Up (https://www.bankdirector.com/magazine/archives/4th-quarter-2021/ransomware-attacks-heat-up/)," also focuses on this growing threat.

Bank Director's 2023 Risk Survey (https://www.bankdirector.com/issues/risk-issues/2023-risk-survey-complete-results/), sponsored by Moss Adams, also explores cybersecurity practices. The survey was conducted in January 2023, and surveyed 212 independent directors, chief executive officers, chief risk officers and other senior executives of U.S. banks below $100 billion of assets.

Emily McCormick is Vice President of Editorial & Research for Bank Director. She oversees research projects, from in-depth reports to Bank Director's annual surveys on M&A, risk, compensation, governance and technology. She also manages content for the Bank Services Program. You can connect with Emily on LinkedIn (https://www.linkedin.com/in/ehmccormick/) or contact her at emccormick@bankdirector.com (mailto:emccormick@bankdirector.com).