SecurityScorecard

farm CREDIT
MID-AMERICA

CASE STUDY

SecurityScorecard 1.800.682.1707 / 214 W29th St, 5th Flr, New York, NY 10001 / sales@securityscorecard.io

The Client

Farm Credit Mid-America ("Farm Credit") is one of the largest agricultural lending cooperatives within the U.S. Farm Credit System, with over 1,100 employees and more than 100,000 customers across Indiana, Ohio, Kentucky, and Tennessee.

As a part of the U.S. Farm Credit System, Farm Credit Mid-America is subject to the rules and regulations put out by the Farm Credit Administration. The FCA, though it is an independent agency, routinely issues guidance that is consistent with the broader federal financial service agencies such as the OCC, FDIC and FFEIC.

As it relates to cybersecurity, the FCA has recommended that its institutions follow FFIEC cybersecurity guidelines including:

- Managing connections with and to third-party vendors;
- Engaging boards of directors and senior management to ensure they understand their institutions' cybersecurity risks; and
- Monitoring and maintaining sufficient awareness of threats and vulnerabilities throughout the organization.

We spoke to Chief Security Officer and Assistant Vice President of Database Systems Mike Everett. Everett has over 18 years of technology experience within the financial services, government and medical industries. His responsibilities at Farm Credit Mid-America include delivery and execution of the organization's overall information security strategy and awareness, as well as production data operations.

The Challenge

According to Everett, Farm Credit has become increasingly attuned to the importance of monitoring the security posture of its third parties. One of the primary concerns is that vendors who are not subject to the same or similar regulatory oversight as Farm Credit may not set as high a standard on security as Farm Credit itself. In a budget- and time-conscious company, a lower minimum standard might mean lower security, which ultimately translates to a potential risk for Farm Credit.

Like so many others faced with the challenge of managing vendor risk, Farm Credit started with an in-house process that was simple and familiar enough to incorporate: an assessment questionnaire. The assessment was sent out to each existing vendor to gauge security status and was also sent to any new vendors as an added level of diligence before the new vendor started doing work for Farm Credit.

> “People are the weakest link, and that’s true for third-parties too.”

For those who have tried this method and found themselves buried in excel sheets and questionnaires, it’s easy to understand how this approach wasn’t the ideal solution for the Farm Credit team. A breakdown of a few of the shortcomings of this approach:

Ineffective Use of Resources: In most cases, the people who are appointed as being responsible for the upkeep and management of these surveys from vendors are not solely dedicated to this role. This means, in nearly every instance, a highly-qualified and potentially highly-paid individual is now spending a significant portion of their time performing administrative functions. At Farm Credit, three experienced security engineers were burdened with tasks like sending reminders to vendors who had not yet filled in the assessment.

Only Reflective of a Point in Time: Simply put, the obvious fault of a point-in-time questionnaire is that it only reflects the security maturity of an organization in one moment. A secure vendor could quickly become a problematic one, and on the other hand, a third party could remediate a few of its security holes and drastically reduce its risk landscape. In both scenarios, the company sending the questionnaires might not be aware till months later. Everett described this issue as having no real time visibility into his growing number of connected vendors.

Maybe, Not Even Reflective: Another rarely-discussed wrinkle added by the point-in-time assessment is that it is inevitably colored by the vendor's desire to keep client business. Even the most responsible, forthcoming vendor has a sales team, a general council, and an account manager who can shift the conversation from "How Should We Disclose This?" to "Should We Disclose This?" The result of the well-intentioned vendor with too much prep time is an assessment riddled with Not Applicable's with little to no information that would allow for a substantive assessment. (Note: We didn't have a chance to discuss this aspect with Everett, but since it's a challenge that companies like Farm Credit are likely to encounter, we've included it in this Case Study.)

Faced with the growing reality that their initial approach was not the right fit, the Farm Credit team set out on a mission to find the solution that would allow them to continuously monitor Farm Credit's vendors in an efficient manner.

The Solution

By adopting the SecurityScorecard platform, Farm Credit Mid-America could finally proactively monitor all of the firm's connected third party vendors. Additionally, other departments that rely on Everett's team for vendor approval have experience a substantial improvement in feedback and turnaround time for new vendor approvals. As the firm's ecosystem of connected vendors continues to grow, the platform's real time & continuous monitoring, along with portfolio organization and notification suite have capability, allowing Everett and his team to identify specific security areas or issues that need remediation.

> "SecurityScorecard has given my team the visibility into our vendor ecosystem and enabled us to be proactive as we manage security risk."

In addition to improving the velocity of vendor onboarding, Everett is now able to now provide regular vendor risk reporting both within his department, across the company and to the firm's internal governance committees and external regulators. Improvements to portfolios can be tracked over time, and easily reported, which allows Everett to communicate the value of his teams practice across the firm. Individual vendor reports can be shared directly with the firm's vendors via online remediation workflows. Farm Credit Mid-America's vendors are given the opportunity to remediate and improve their scores, which allows Everett to not only assess, but monitor and improve his ecosystem's risk profile.

> "SecurityScorecard's platform has allowed to completely transition from paper assessments, unlocking tremendous resource leverage within the security team."

The Results

Everett has dramatically improved his team's capacity while substantially improving the new vendor experience for other department heads. SecurityScorecard reports create a medium of communication that allows the team to explain why certain vendors are a great risk than others. This is especially helpful when the team interacts with departments that don't have the technical background of Everett's team.

Self-monitoring, also allows Everett's to keep track of the firm's own attack surface and ensures his team remains abreast of potential issues. When assessing new third-parties, Everett's team uses SecurityScorecard to identify problematic vendors, while also providing alternative options through the platform's vendor comparison tool. The platform's real time monitoring and notification tools ensure the team is always aware of changes within their portfolios.

> "SecurityScorecard absolutely saves my department time, and has substantially improved visibility of risk within our vendor ecosystem."

Conclusion

Everett and his team are now working on new policies and process where fluctuations in a vendor's security score will trigger certain events. If a vendor grade suddenly falls, the platform will alert the team to take remedial action.

Farm Credit has easily been able to demonstrate to its proactive security practice to governance committees and regulators. On a broader scale, use of SecurityScorecard has elevated awareness, appreciation and ascribed value to Everette's team and their efforts to keep Farm Credit secure in a meaningful way.

"As a CISO, I always have to think 'are we doing the right thing to keep our data, our customer's data and our employees safe?"