SecurityScorecard

CASE STUDY

Large Agricultural Lending Cooperative Enhances Internal & External Cybersecurity Posture Utilizing SecurityScorecard

SecurityScorecard.com
info@securityscorecard.com

Tower 49
12 E 49th St
Suite 15-001
New York, NY 10017
1.800.682.1707

THE CLIENT

As one of the largest agricultural lending cooperatives within the United States, employing over 1,000 individuals and working with more than 100,000 customers, this client is subject to the rules and regulations put out by the Farm Credit Administration (FCA). As an independent agency, the FCA will routinely issue 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 with the company's Chief Security Officer, also serving as the Assistant Vice President of Database Systems. The individual has over 18 years of technology experience within the financial services, government and medical industries. Their responsibilities within the company include delivery and execution of the organization's overall information security strategy and awareness, as well as production data operations.

THE CHALLENGE

According to this CISO, the company 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 may not be subject to the same or similar regulatory oversight, may not set as high a standard on security as they themselves. In a budget- and time-conscious company, a lower minimum standard might mean lower security, which ultimately translates to a potential risk for the company.

Like so many others faced with the challenge of managing vendor risk, the company 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 them.

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 company's team. Here is a breakdown of a few of the shortcomings to 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. For this client, 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. The CISO described this issue as having no real time visibility into their 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", with little to no information that would allow for a substantive assessment.

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

THE SOLUTION

By adopting the SecurityScorecard platform, the client found they could proactively monitor all of the firm's connected third party vendors. Additionally, other departments that rely on the CISO's team for vendor approval have experienced 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 the CISO and their team to identify specific security areas or issues that need remediation.

In addition to improving the velocity of vendor onboarding, the CISO is now able to now provide regular vendor risk reporting both within their 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 the CISO to communicate the value of their team's practice across the firm. Individual vendor reports can be shared directly with the firm's vendors via online remediation workflows. The company's vendors are given the opportunity to remediate and improve their scores, which allows the CISO to not only assess, but monitor and improve their ecosystem's risk profile.

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

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

THE **RESULTS**

The CISO has dramatically improved the 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 greater risk than others. This is especially helpful when the team interacts with departments that don't have the technical background of the CISO's team.

Self-monitoring also allows the CISO to keep track of the firm's own attack surface and ensures the team remains abreast of potential issues. When assessing new third-parties, the CISO'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

The CISO and their team are now working on new policies and processes, 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.

The company has easily been able to demonstrate its proactive security practice to governance committees and regulators. On a broader scale, use of SecurityScorecard has elevated awareness, appreciation and ascribed value to the CISO's team and their efforts to keep the company 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?"

ABOUT SECURITYSCORECARD

Funded by world-class investors including Silver Lake Partners, Sequoia Capital, GV, Riverwood Capital, and others, SecurityScorecard is the global leader in cybersecurity ratings with more than 12 million companies continuously rated. Founded in 2013 by security and risk experts Dr. Aleksandr Yampolskiy and Sam Kassoumeh, SecurityScorecard's patented rating technology is used by over 25,000 organizations for enterprise risk management, third-party risk management, board reporting, due diligence, and cyber insurance underwriting. SecurityScorecard continues to make the world a safer place by transforming the way companies understand, improve and communicate cybersecurity risk to their boards, employees and vendors. Every organization has the universal right to their trusted and transparent Instant SecurityScorecard rating.

FOR MORE INFORMATION, VISIT SECURITYSCORECARD.COM OR CONNECT WITH US ON LINKEDIN.

SecurityScorecard.com
info@securityscorecard.com

Tower 49
12 E 49th St
New York, NY 10017
1.800.682.1707

SecurityScorecard