Cyber Insurance for Agriculture

Sarah Sellars, Assistant Professor & SDSU Extension Sustainable Farm & Food Systems Specialist
Ali Mirzakhani Nafchi, Assistant Professor & SDSU Extension Precision Agriculture Specialist
Sushant Mehan, Assistant Professor & SDSU Extension Water Resource Engineer Specialist
Logan Vandermark, SDSU Extension Precision Livestock Field Specialist
Jameson Brennan, Assistant Professor & SDSU Extension Livestock Grazing Specialist
Xufei Yang, Assistant Professor & SDSU Extension Environmental Quality Engineer

August 2024

Introduction

Like any business, farms and agricultural operations are vulnerable to cyber-attacks. According to the Food and Agriculture – Information Sharing and Analysis Center (Food and Ag-ISAC), in 2023, there were 167 ransomware attacks on the food and agriculture sector globally, accounting for 5.5% of the total volume of ransomware attacks. The food and agriculture sector is the 7th most attacked sector of the 11 sectors that are monitored (Food and Ag-ISAC, 2024). As farmers and ranchers have adopted more precision agriculture technologies over time and will continue to do so, they must consider how to protect this valuable data that is essential for their operations.

Insuring Cyber Risk

With the increase in the use of precision agriculture, farms and ranchers are becoming more vulnerable to cyber-attacks. Hackers can hold farm data for ransom. From 2019 to 2020, the average ransom demand doubled, with the highest observed ransom demand at $23 million (FBI, 2021). In January 2021, a ransomware attack against a farm caused $9 million in losses from shutting down their farming operations (FBI, 2021). Other risks for farm data besides data theft include ransomware and data destruction. Ransomware can be used to make files unreadable, and data destruction could result in the loss of valuable farm data (FBI, 2016).

Cyber-attacks are risky because they can cause farmers, ranchers, or business owners to possibly incur enormous, unexpected costs. One way to mitigate this risk is by using cyber insurance. Cyber insurance can cover farmers for the risk of a data breach, cyber extortion, or identity restoration. Typically, there are two types of cyber insurance offered: first-party and third-party coverage. First-party coverage would directly cover the policyholder's losses from a data breach on their own data system or network. Third-party coverage covers the policyholder if a third party brings claims against them due to a data breach (FTC). For example, if you have a small business and your client information was hacked and published online, third-party coverage will protect you from legal costs if your client decides to sue you due to their leaked information.

For farmers and ranchers, first-party coverage would be the most useful option unless they are also business owners who are storing client data. Some recommendations are to ensure that the cyber insurance policy covers data breaches, cyber-attacks on your data held by third parties, cyber-attacks from breaches in your network, and cyberterrorism (FTC). Some companies offer cyber insurance policies specifically for farmers and ranchers. For example, AmericanAg offers policies to cover first and third-party data breaches, cyber extortion, and identity restoration (AmercianAg). Nationwide also offers cyber security insurance and promotes the policy for farmers (Nationwide).

Conclusion

While cyber insurance may not be widely adopted at the producer level yet, producers may want to learn more about it, especially if they have precision-intensive operations. Crop and livestock farms that are at high risk for losses from data breaches or operational disturbances may want to consider a policy. Producers are encouraged to follow proper protocols for storing, managing, and securing data to help protect themselves from cyber-attacks.

References

AmericanAg. 2024. "Commercial/Farm Cyber Coverage." aaic.com/reinsurance/farm-bureau-reinsurance/farm-bureau-products/specialty-products/commercial-farm-cyber-coverage/

Food and Ag-ISAC. 2024. "Farm-to-Table Ransomware Realities." foodandag-isac.org/_files/ugd/473ff0_c3dc3a5c53d44cefb9c123640275b029.pdf

FBI. 2021. "Cyber Criminal Actors Targeting the Food and Agriculture Sector with Ransomware Attacks." Private Industry Notification. Pin No: 20210901-001. ic3.gov/Media/News/2021/210907.pdf

FBI. 2016. "Smart Farming May Increase Cyber Targeting Against US Food and Agriculture Sector." Private Industry Notification. Pin No: 160331-001. info.publicintelligence.net/FBI-SmartFarmHacking.pdf

Federal Trade Commission. n.d. "Cyber Insurance." ftc.gov/business-guidance/small-businesses/cybersecurity/cyber-insurance

Nationwide. n.d. "Prioritizing Cybersecurity on Farms." nationwide.com/lc/resources/farm-and-agribusiness/articles/cybersecurity-farms

South Dakota State University Extension

SOUTH DAKOTA STATE UNIVERSITY®
NESS SCHOOL OF MANAGEMENT AND ECONOMICS

Learn more at extension.sdstate.edu.

P-00306