

Ripe for the Picking: Hackers Target Agribusinesses

Written By **Peter N. McClelland, CIPP/US** (pnmcclelland@wardandsmith.com) and **Allen N. Trask, III** (ant@wardandsmith.com)

April 30, 2021



Agribusiness may not be an industry that the public at large often associates with data breaches and hacking, but whatever the perception may be, the agricultural sector of the American economy is increasingly a ripe target for malicious foreign actors, digital fraud, and

other perpetrators of cybercrime.

These threats will only increase as Precision Agriculture—the greater incorporation of digital and satellite systems into agricultural production—and software based on machine learning take greater prominence in the agricultural sector.

According to the Ponemon Institute's survey of data breaches in 2020, the average all-in cost of a data breach globally was \$3,860,000, but in the United States the number was much higher at \$8,640,000, making American businesses—by far—the most aggrieved group from a data breach perspective. There was about a 5.5% increase in the average cost compared to last year, so this problem is unlikely to do anything but worsen in the years to come. Legal costs alone average hundreds of thousands of dollars, and attorneys' fees will only be a piece of that figure.

As a Department of Homeland Security report on Threats to Precision Agriculture notes, "data theft, stealing resources, reputation loss, destruction of equipment, or gaining an improper financial advantage over a competitor," are all threats that the American agricultural industry will continue to face in a digitizing world. And indeed, wire fraud, stealing financial credentials and stealing competitors' intellectual property are all significant concerns for Agribusiness today.

However, the same report by the Ponemon Institute that found such high costs associated with data breaches also found that some basic steps implemented before a breach occurs will—on average—reduce the cost of a data breach drastically, and—perhaps surprisingly—few of the most important steps need to involve large investments in high-tech systems. Rather those steps often principally involve planning and getting the right training to the people who make up an organization.

First, having an incident response plan and testing it will, on average, reduce a data breach's cost by about 15%. A business continuity plan will reduce the average cost by 7.22%. And employee training will reduce the

average cost by about 6.17%, which is more than the 6.14% that extensive encryption will save. By contrast, migrating information to the cloud without proper insurance and contractual protections will increase the average cost by more than 7.5%. Compliance failures will—on average—increase costs by 6.6%, and interconnected devices (sometimes called the internet of things) which are powering advances in agricultural technologies can increase the average cost of a data breach by over 5%. These percentages in the abstract may seem small until we remember that they are being applied to a typical breach, with costs that reach several million dollars.

Technology has always driven the American agricultural sector forward, and it will continue to do so for years to come. But the increasing digitization of the agricultural workspace and the implementation of new agricultural technologies open a business up to enormous losses if they do not plan ahead for the future. At Ward and Smith, we want to help you secure your company's future by planning for that future and giving your team the tools they need to avoid the pitfalls any change naturally brings. There are no magical solutions or silver bullets, but with our team's expertise in Privacy and Data Security and your knowledge of your organization, you will be set up to succeed today and in the future.

--

© 2021 Ward and Smith, P.A. For further information regarding the issues described above, please contact Peter N. McClelland, CIPP/US or Allen N. Trask, III.

This article is not intended to give, and should not be relied upon for, legal advice in any particular circumstance or fact situation. No action should be taken in reliance upon the information contained in this article without obtaining the advice of an attorney.

We are your established legal network with offices in Asheville, Greenville, New Bern, Raleigh, and Wilmington, NC.