CYBERCRIME TAKES AIM AT AMERICA'S FOOD SUPPLY

By **Victoria G. Myers, @myersPF**

You'll never see their faces, but high-tech criminals lurk far beyond the farmgate. Their intent is to cause chaos and financial loss for America's farmers and ranchers. The risk has only heightened as agriculture becomes increasingly digitally interconnected with the country's food supply and transportation networks.

"These attackers used to go after the Amazons and banking institutions of the world, but now they are looking at different companies, specifically those in agriculture and energy," says Sarah Engstrom, chief information security officer and vice president of information technology (IT) security, productivity and privacy for CHS.

One of the most public breaches affecting agriculture this year has been against JBS USA, a processor responsible for production of about one-fifth of the nation's meat supply. The company was forced to halt slaughter operations in 13 meat-processing plants and reported it paid $11 million to hackers to regain control of its systems. This happened despite the fact JBS USA spends more than $200 million annually on IT and employs more than 850 IT specialists around the world.

Engstrom is in the IT trenches every day for CHS, a diversified and global agribusiness cooperative organized in 1929 and headquartered in Minnesota. She did not shy away when asked to talk about the challenges large entities such as CHS face from cyberattackers.

"They are looking for targets they believe are more prone to caving under an attack or to being exploited and not having the proper security resources in place," she says. "We are seeing it, and we are hearing of smaller companies getting pummeled with cyberattacks and ransomware."

Fighting cybercrime isn't as simple as installing a new lock and chain. Cybercriminals are high-tech crooks, constantly changing the tools of their trade. It's far from a new line of work. Considered the first electronic bank robbery by many in law enforcement, Russian computer

GETTY IMAGES

programmers working out of St. Petersburg hacked into the systems of a major U.S. bank in 1994 and started skimming money. The group made away with more than $10 million before the bank became aware of the intrusion.

IT'S NOT IF BUT WHEN

Today, for many in IT, a data breach has become more of a "when" than a "what if" scenario. According to the FBI's 2020 "Internet Crime Report," the agency received 791,790 cybercrime complaints in 2020, with losses of more than $4.1 billion. That is a 69% increase from year-earlier levels. The FBI reports attackers are increasingly using tools like machine learning, artificial intelligence and even the 5G mobile network to ramp up offenses.

The website GearBrain, which tracks data breaches and hacks, reported that in the first quarter of 2021, the number of people impacted by data breaches climbed 564% compared to year-ago levels. The number of compromised companies in the U.S. were up 12% during that same period. The report says the "rise in supply chain attacks is troubling." Some IT specialists believe one reason for the increase is because more employees are working from home, where they are not always connected to more secure company computer networks.

PREPARING FOR BATTLE

Agribusiness giants like ADM understand the threat hackers pose to their operations.

"We assume we will be a target. That is the safer position to take," Archer Daniels Midland Co. (ADM) president and CEO Juan Luciano stressed at a recent *Wall Street Journal* Global Food Forum.

Luciano explained the company's security is built around strategies for risk management, having redundancies and providing multiple sources for customers. They have a ransomware task force, retain cybersecurity experts and work with employees to create an awareness of common ways hackers gain access to a company.

"We have been in business 119 years. We've been through wars, hurricanes and a pandemic, and we kept 800 plants running and operating," Luciano said. "We own rail yards, barges, trucks, ocean-going vessels. We have multiple locations. If you can't go to one elevator, you can go to another. We can divert rail or trucking. We are not completely invulnerable, but we feel good about our level of protection."

THERE ARE NO GUARANTEES

Farmers and ranchers are increasingly sharing operation and personal data through a variety of online platforms. What happens when an online supplier is hacked, and seed or inputs are suddenly inaccessible when they are most needed? What about commodity markets? Transportation networks?


Sarah Engstrom

Redundancies and optional suppliers and buyers seem to be one of the best protections available today. Analysts stress the importance of building redundancies into every segment of an operation.

CHS's Engstrom says smaller companies are often not always in a strong cybersecurity position because of limited financial resources.

"In today's digital age, cybersecurity is a necessary place to invest if you are going to take a proactive or reactive posture. It's unfortunate, but many people still have a mindset that you can implement technology, set it and forget it. That is no longer an option. We have to move past that kind of thinking."

Asked if precision agriculture and specialty-market data sharing are opening up more operations to potential attacks, Engstrom says the more interconnected we are in agriculture, the more opportunity it gives cyberattackers to do their dirty work.

"What a farmer or rancher can do right now to protect their operations and their data is to spend time and thought, and have a conversation with any provider that is supposed to be securing their data. Ask if that entity is, in fact, investing in security. Ask them what attacks they can combat, how and what's on their road map to continually mature. There is no going back. There is only asking the right questions and evaluating the security posture of whatever organizations we agree to do business with."

GOVERNMENTAL PROTECTIONS

Efforts to interview officials in the U.S. Department of Agriculture regarding cybersecurity were met with nonresponses. Yet, there is clearly awareness of the issue based on Executive Order 14017, issued by President Joe Biden in February of this year.

The order tasked heads of federal agencies to report to the President on the strength and resilience of America's supply chains. Secretary of Agriculture Tom Vilsack and his department were ordered in consultation with the heads of appropriate agencies to "submit a report on supply chains for the production of agricultural commodities and food products."

All reports ordered were to include a review of the "defense, intelligence, cyber, homeland security, health, climate, environmental, natural, market, economic, ➤

IMAGES

geopolitical, human rights or forced labor risks, or other contingencies that may disrupt, strain, compromise or eliminate the supply chain, including risks posed by supply chains' reliance on digital products that may be vulnerable to failures or exploitation ..."

In response to publication of that Executive Order and a call for public comments, Jennifer van de Ligt, director of the Food Protection and Defense Institute at the University of Minnesota, outlined concerns about what she called "significant cybersecurity-related risks to the agricultural and food products supply chain that threaten its resilience and companies and consumers nationwide."

GETTY IMAGES

The Institute addresses vulnerabilities in the global food system with what it calls a "comprehensive, farm-to-table view." It partners with industry, government and academic stakeholders to help assure product integrity, supply chain resilience and brand protection.

Ligt said in a public letter that the Institute saw considerable risk of disruption, strain and compromise from vulnerability to cyberattacks on industrial control systems used in agricultural production, agricultural and food processing, and manufacturing. She pointed specifically to vulnerabilities built into systems and a lack of awareness among executives, equipment operators and regulators of risks.

Ligt wrote that potential consequences would include disruption in availability of agricultural and food products, injury and death to livestock, and even the release of unsafe foods into the market that sicken consumers and damage company brand reputations. ➤

Safeguards Against Cyberattacks

Chief information security officer and vice president of information technology (IT) security for CHS Sarah Engstrom provides practical steps anyone can take to help safeguard his or her information and stymie hackers.

1 Employee/Personal Email. Scams are rampant and are a primary way hackers access data. Email traditionally is "single factor" entry, meaning username and password are all that's required to let the user in.
☑ **Safer Way =** Multifactor authentication using authenticator apps through cell phones or other devices.

2 Device Hygiene. System updates are often released to patch a security issue. The old way was to set it and forget it when it came to technology.
☑ **Safer Way =** Make updates as they come available. This is known as "patching." When a system is old and no longer updates its major operating systems, consider replacing the device.

3 Business Owners Need To Know. Assuming your data and connections are secure is a mistake in today's environment.
☑ **Safer Way =** Have a conversation monthly or quarterly with your organization's IT team, or any third-party entities with whom you share data. Ask if they are spending to secure their platforms, whether they have been hacked and what they have in place to combat future threats.

4 Rethink Insurance. Insurance isn't just for your house, car or crops anymore. More and more claims are being filed with insurance companies over cyberattacks and the damage related to them; in some cases, insurers refuse to indemnify for these losses.
☑ **Safer Way =** Business owners need to talk to insurance providers and know if they are covered for losses in the event they are hacked. If you don't like the answer your insurer gives you, investigate coverage that will, in fact, cover losses from cyberattacks.

5 Incident Response Teams. You never know you need this—until you do. Incident response companies are called in usually prior to paying any type of ransom to assess the situation. Sometimes, cyber criminals will claim they stole data when they did not take anything of importance. Maybe the whole thing is a bluff, or you have enough redundancies built in that you can work around the threat. Incident response firms are overwhelmed, however, due to the escalating number of cyberattacks. They will prioritize customers with existing contractual relationships.
☑ **Safer Way =** Talk to your insurer about incident response firms they use and would recommend. Look into the cost of a contract with one of those firms to give you a faster response in the event you are hacked.

Passwords Matter. Avoid weak passwords, especially those that include family or pets' names, or places of birth.

Her words seem prophetic in retrospect. Ligt's attempts to alert authorities, addressed to Melissa Bailey, of the USDA's Agricultural Marketing Service, were dated March 18, 2021. Less than two weeks later, JBS USA announced it had been hacked.

CHS cybersecurity expert Engstrom is hopeful there will be positive and proactive moves in the future at the governmental level to combat these ongoing cyberattacks. For now, however, she says we can't count on the government alone to protect agriculture against cybercriminals.

"I sincerely hope they are part of a future solution to these problems, but we can't hold our hats and twiddle our thumbs and wait," Engstrom warns. "Private entities will have to invest, ask questions and accept that interconnected systems are part of almost everyone's business today. We have to be prepared to protect ourselves and what we've worked so hard to create."

SECURING PRECISION AG DATA

Can U.S. farmers and ranchers take advantage of the benefits precision agriculture offers and still be assured their data is protected?

PHOTO: MATTHEW WILDE, PHOTO ILLUSTRATION: BARRY FALKNER

Two-Factor Authentication. This is one of the best ways to verify it's really you trying to log in to important financial accounts.

One well-known precision ag business linking producers and their data with the rest of agriculture is Trimble. Cory Buchs, director of Trimble's Connected Farm Platform, understands concerns farmers have about companies' abilities to protect that data. >

Precision Ag Threats

In 2018, 11 team members from the U.S. government and private sector outlined threats as they perceived them in a public-private analytic exchange program: "Threats to Precision Agriculture." Key risks they identified included:

Threats to Confidentiality. Data privacy in the areas of crop yields, land prices and even animal herd health were spotted as concerns. The report noted that loss or misuse of data could have financial and emotional impacts at the farm level, and there could also be a loss of reputation and business for both equipment and software manufacturers in the event of a breach. Areas the group noted were especially treacherous included the use of decision support systems that could, by design, be malicious and steal data; intentional publishing of confidential information, such as market data, from within an industry to cause chaos; and even foreign access to unmanned aerial systems. The group identified at least one threat where a company was approached with offers to sell data under the table to commodity brokers or hedge funds.

Threats to Integrity. Here, the group considered how "smart farming" could be manipulated. It pointed to intentional falsification of data to disrupt crop or livestock sectors, even to the point of planting false data that mimicked actual reports prior to or during a livestock disease outbreak. The same could apply to crops. Smart sensors could be used to disrupt automation systems and HVACs, potentially damaging stored crops or resulting in adverse health impacts to animals.

Threats to Availability. As farmers and ranchers rely on their equipment, the timing of its availability to them could lead to damage or a failure to meet optimal planting or harvest windows. Malicious actors, the report noted, could possibly identify a vulnerable type of equipment and disrupt thousands of machines at once. There is a related concern that GPS signal access could be denied, and rural cellular and broadband networks continue to be a weak point for agricultural security.

To read the full report, visit:

> **www.dhs.gov/sites/default/files/publications/2018%20AEP_Threats_to_Precision_Agriculture.pdf**

Antivirus Protection. Keep it up-to-date and turned on. Also, check to see that your firewall is switched on.

"Carbon credits, collecting data to help make better decisions ... all of these type things provide value. We can't let the value overwhelm the importance of having security around the collection process. Rather, it's that very value that makes securing this data all the more important, especially as we interact with third parties and move data from devices, storage in the cloud, etc."

Buchs says there is a lot a company like Trimble can do to protect farmers' data, but there is also a need for all of agriculture to do a better job to educate about best technology practices on the farm.

"I think trends today tell us we will see more attempts at hacking," he says. "That should only increase a company's determination to stay ahead of those threats. It's kind of a race of sophistication on both sides. If you're a farmer, you have to ensure you only trust data to someone willing to invest in security protocols, processes and tools that are current and will ensure the security of your data. We do that at Trimble, and most of the larger, more established companies in the ag space do, as well."

Backups Are Critical. Make regular backups of data using external hard drives, the cloud or both.

Buchs cautions it's sometimes more of a risk to work with startup businesses, where there may be fewer resources available to invest in security protocol. He says companies should be transparent when asked by users, or potential users, about processes and procedures they employ for security. There are also resources to help laypeople evaluate companies, including online sources to see companies that have been hacked.

Buchs notes the best companies have put into place tools for immediate intrusion detection and vulnerability-scanning analytics. They rely on tools including multifactor authentication, which he says is a proven way of protecting client data at the first line of attack. These protocols require more than one device to log in.

In Trimble's case, Buchs adds, cybersecurity has benefited from being part of a larger global company with divisions outside of agriculture in the construction and geospatial industries, which have similar challenges to solve.

Reputable companies, he stresses, make it a point to invest in security, and they have backups. "Given the value of a farm's data, it's critical to have backups and to be able to recover data if something happens."

So what about recovery? Is it days, weeks? In the case of Trimble, Buchs says it's minutes to hours. "We operate in the cloud and have access readily. For us, recovery is not a long process."

Encryption. Consider this as another layer of protection. The option is built into most PCs and Macs, and prevents unauthorized access.

THE CLOUD IS NOT A SHIELD

To be clear, having your data in the cloud is not a complete, or bulletproof, solution. Unfortunately, the cloud is hackable, too.

"In general, anything is hackable that's connected to the internet," Buchs explains. "That's the inherent risk when connecting to the cloud. But, companies like Trimble have invested in ensuring security and ensuring safety of that traffic.

"Data from your Trimble devices and cloud is encrypted and behind a firewall, where it is monitored for intrusion," he continues. "In addition, other sophisticated methods are applied to ensure its security. There are always risks, and I think for agriculture, the threat has increased. We have to constantly have security at a high level. That isn't going to change."

When it comes to precision ag, it's not always the data cybercriminals are after. Often, it's the technology itself that has the value, Buchs explains. He says hackers are often trying to steal trade secrets to sell outside of the U.S. in an effort to propel foreign companies to America's technology level without investing the expense and time.

"In agriculture, there is a real-world incentive," he continues. "Not only is there a lot of money involved, but we are talking about food—a major requirement for life and a source of stability. These are high stakes, and we have to stay ahead of the threat on a constant basis." ///

You Can't Be Too Nice. Phone calls or emails from people you don't know should be viewed with caution. Never click on a link in an email you are not expecting. Never share personal information over the phone. If you have doubts about the authenticity of correspondence, check directly with your financial institution or your local police department.