ACCESS DENIED: THE DANGERS OF RANSOMWARE'S UNCHECKED ATTACK ON THE AGRICULTURE INDUSTRY

Madeline E. Hartley†

I. Introduction 458
II. What is Ransomware? 459
A. Who Are the Players Behind Attacks? 460
B. How Do Criminals Attack? 461
III. Not a New Threat to Agriculture 462
A. The USDA's Vulnerabilities as a Federal Agency 462
B. The Agriculture Industry as a Target 463
C. Precision Agriculture & Producer Level Vulnerabilities 466
IV. The Biden Administration's Response to Increased Cyber Security Threats 468
V. Remaining Gaps in the Regulatory Landscape 470
A. Shut Down Illicit Actors Through Enforcement of Already Enacted Federal Statutes 471
B. Develop Mandatory, Agriculture-Specific Data Security Regulations 472
C. Hold the USDA Accountable 472
VI. Private Action Will Aggregate 473
A. Strengthen Passwords & Utilize Multi-Factor Authentication 473
B. Should a Ransom Be Paid? Important Legal Considerations if Considering Making a Ransomware Payment 475
1. Ransomware Payments Enable Criminal Activity, Threaten United States National Security Interests, and May Violate OFAC Regulations 476
2. Ransomware Attacks may Impose Liability Under the Bank Secrecy Act, and Anti-money Laundering Laws 477
C. Individuals or Organizations Should Plan for an Attack and Know How to Respond if One Occurs 478
VII. Conclusion 479

† J.D. Drake University Law School, May 2023; B.S. Agricultural Business, May 2020, Iowa State University. The Author dedicates this Note to her family, who demonstrate a dedication and love for the land that has survived over four generations. The author would like to thank her family, especially her husband, for their continued love and support. Special thanks to the *Journal* staff for their superb editorial work on this piece.

I. INTRODUCTION

Ransomware attacks occur every eight minutes and present a serious threat to our nation's security, economy, and food supply.[1] The COVID-19 global pandemic has further exacerbated deficits in cybersecurity and increased the threat of cyberattacks as more institutions shift to virtual work.[2] Ransomware poses an increased risk to the agriculture sector, which produces critical outputs for other industries.[3] The risk is not hypothetical in nature—the Federal Bureau of Investigation (FBI) has warned of cyber criminals' intentions to *explicitly* target the agriculture industry.[4]

Congress has a long-standing history of supporting the food and agriculture industry, most notably through the Farm Bill.[5] The first Farm Bill was enacted in 1933 during the Great Depression and Dust Bowl era.[6] Although the Farm Bill has changed drastically and is now more expansive in nature, the law illustrates just how integral the agriculture industry is to the United States economy.[7] Today, food, agriculture, and related industries contribute nearly $1.1 trillion to the United States' gross domestic product (GDP).[8] In 2020, over 19.7 million jobs were related to the agriculture and food sectors, representing 10.3% of total United States

1. Rich Barlow, *Why Are Ransomware Attacks Happening So Often–and Can They Be Stopped?*, BU TODAY (June 8, 2021), https://www.bu.edu/articles/2021/why-are-ransomware-attacks-increasing/ [https://perma.cc/VEA4-WQ67].

2. FED. BUREAU OF INVESTIGATION INTERNET CRIME COMPLAINT CTR., INTERNET CRIME REPORT 2020 3 (2020), https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf [https://perma.cc/E85W-Y9ZM].

3. FED. BUREAU OF INVESTIGATION CYBER DIV., PIN. NO. 20210901-001, CYBER CRIMINAL ACTORS TARGETING THE FOOD AND AGRICULTURE SECTOR WITH RANSOMWARE ATTACKS 2 (2021), https://www.ic3.gov/Media/News/2021/210907.pdf [https://perma.cc/Q4Q2-T9FS] [hereinafter CYBER CRIMINAL ACTORS].

4. *See id.* (emphasis added).

5. *See generally* CONG. RSCH. SERV., RS22131, WHAT IS THE FARM BILL? (2019), https://crsreports.congress.gov/product/pdf/RS/RS22131 [https://perma.cc/8F3V-AUFW] [hereinafter WHAT IS THE FARM BILL?]. The first Farm Bill was passed in 1933 providing subsidies and other controls to help raise farm income and promote conservation. *Id.* at 4. The first omnibus Farm Bill passed in 1973. *Id.* The Farm Bill provides policy makers an opportunity to address agricultural issues comprehensively and systematically. *Id.* at 1. The last Farm Bill contains 12 titles "encompassing commodity revenue supports, farm credit, trade, agricultural conservation, research, rural development, energy, and foreign and domestic food programs, among other programs." *Id.*

6. *Id.* at 4.

7. *Id.* at 1.

8. *Ag and Food Sectors and the Economy*, U.S. DEP'T OF AGRIC. ECON. RSCH. SERV. (Feb. 24, 2022), https://www.ers.usda.gov/data-products/ag-and-food-statistics-charting-the-

employment.[9] In the most recent version of the Farm Bill – The Agriculture Improvement Act of 2018 – the Congressional Budget Office (CBO) estimated the total cost of the Farm Bill's mandatory programs would be $428 billion over its five-year duration.[10]

It is undeniable that supporting the agriculture industry is still very important to this nation's people and government.[11] Why, then, are we are willing to invest hundreds of billions of dollars in such a vital industry but leave it exposed to the egregious risk posed by ransomware?[12] Continuing to leave the agriculture industry exposed to the risk of ransomware attacks is nothing short of reckless.

II. WHAT IS RANSOMWARE?

Ransomware is a malicious software or malware that encrypts data while blocking access to, or recovery of, data until the owner has paid a ransom.[13] If a ransom is not paid, the victim's data remains unusable.[14] Frequently, cyber criminals pressure victims into acting fast by threatening to publish sensitive data or even destroy data if victims do not comply.[15]

In 2021, the Internet Crime Complaint Center (IC3) received 3,729 complaints identified as ransomware incidents, resulting in loss of more than $49.2 million.[16] This is over a 50% increase in incidents from the year prior and a loss of an additional $20 million in economic damages.[17] Since early 2018, the frequency of broad-based ransomware attacks has decreased.[18] Unfortunately, according to

essentials/ag-and-food-sectors-and-the-economy/?page=1&topicId=b7a1aba0-7059-4feb-a84c-b2fd1f0db6a3 [https://perma.cc/GDS2-3DEX].

9. *Id.*

10. WHAT IS THE FARM BILL?, *supra* note 5, at 4.

11. *See id.* at 1.

12. *See id.* at 4.

13. DEP'T OF THE TREASURY, ADVISORY ON POTENTIAL SANCTIONS RISKS FOR FACILITATING RANSOMWARE PAYMENTS 1 (2020), https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf [https://perma.cc/PSC8-PDKD] [hereinafter ADVISORY ON POTENTIAL SANCTIONS].

14. INTERNET CRIME REPORT 2020, *supra* note 2, at 14.

15. *Id.*

16. FED. BUREAU OF INVESTIGATION INTERNET CRIME COMPLAINT CTR., INTERNET CRIME REPORT 2021 14 (2021), https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf [https://perma.cc/B2BQ-VHM3].

17. *See* INTERNET CRIME REPORT 2020, *supra* note 2, at 14 (In 2020, IC3 recorded over 2,474 ransomware incidents, resulting in cumulative losses of over $29.1 million); *see also* INTERNET CRIME REPORT 2021, *supra* note 16.

18. FED. BUREAU OF INVESTIGATION, I-100219-PSA, PUBLIC SERVICE ANNOUNCEMENT:

the FBI, attacks are becoming more targeted, sophisticated, and expensive for victims.[19]

Ransomware attacks have become more commonplace and are an expected cost for state and local governments, healthcare facilities, and companies, of which are the most targeted "persons."[20] Globally, the average ransomware payments per incident among all sectors is $1.85 million; this figure does not account for the value of downtime, labor, lost opportunity, and other transaction costs.[21]

A. Who Are the Players Behind Attacks?

Some of the most notable ransomware groups are believed to be operating in Russia.[22] However, Iran, China, and North Korea are also key players.[23] There is even evidence indicating Iranian government organizations have been involved in a ransomware campaign through a contracted third party.[24] Further, in February of 2021, three North Korean military hackers were indicted by the Department of Justice (DOJ) for a scheme to commit cyber-attacks and financial crimes, including plans to extort more than $1.3 billion.[25] The countries where the majority of attacks originate is problematic—the United States has multiple sanctions already in place

HIGH-IMPACT RANSOMWARE ATTACKS THREATEN U.S. BUSINESSES AND ORGANIZATIONS (2019) [hereinafter PUBLIC SERVICE ANNOUNCEMENT]; *see generally* INTERNET CRIME REPORT 2021, *supra* note 16 ("Ransomware tactics and techniques continued to evolve in 2021, which demonstrates ransomware threat actors' growing technological sophistication and an increased ransomware threat to organizations globally.").

19. PUBLIC SERVICE ANNOUNCEMENT, *supra* note 18.

20. *Id.*

21. *Ransomware Trends 2021*, DEP'T OF HUM. & HEALTH SERVS. CYBERSECURITY PROGRAM 11 (June 6, 2021), https://www.hhs.gov/sites/default/files/ransomware-trends-2021.pdf [https://perma.cc/T5LR-NA8R].

22. Sean Lyngaas, *Suspected Iranian Hackers Pose as Ransomware Operators to Target Israeli Organizations*, CYBERSCOOP (May 25, 2021), https://www.cyberscoop.com/iran-ransomware-israel-sentinelone/ [https://perma.cc/2QCS-6HGY].

23. *Id.*; *Three North Korean Military Hackers Indicted in Wide-Ranging Scheme to Commit Cyberattacks and Financial Crimes Across the Globe*, U.S. DEP'T OF JUST. OFF. OF PUB. AFFS. (Feb. 17, 2021), https://www.justice.gov/opa/pr/three-north-korean-military-hackers-indicted-wide-ranging-scheme-commit-cyberattacks-and [https://perma.cc/G6C4-TGHA] [hereinafter *Three North Korean*].

24. Lyngaas, *supra* note 22; *A Second Iranian State-Sponsored Ransomware Operation "Project Signal" Emerges*, FLASHPOINT (Apr. 30, 2021), https://www.flashpoint-intel.com/blog/second-iranian-ransomware-operation-project-signal-emerges/ [https://perma.cc/76U2-DMXJ].

25. *Three North Korean*, *supra* note 23.

and more sanctions are unlikely to be persuasive to discontinue the prohibited activity.[26]

B. How Do Criminals Attack?

Cyber criminals use a variety of techniques to infect their victims' technology. The FBI reports hackers are routinely using high-tech tools such as machine learning, artificial intelligence, and 5G networks.[27] Common techniques used to infect victims with ransomware include email phishing campaigns, Remote Desktop Protocol vulnerabilities, and software vulnerabilities.[28]

After a security breach has occurred, ransom is often requested in the form of cryptocurrency, such as Bitcoin, because it is not easily traceable. Cryptocurrency has been a key contributor to the growth of the ransomware industry because of its "ease, anonymity, and speed."[29] Cryptocurrency is a key component of ransomware attacks because it makes it easier to remain anonymous when transferring a ransom payment.[30] Because cryptocurrencies like Bitcoin lack a discernable audit trail and operate outside of regulated financial networks—there is no central bank or Federal Reserve and virtually no government surveillance or regulation.[31]

In September 2021, SUEX OTC, S.R.O (SUEX), a virtual currency exchange, was sanctioned by the United States government for its part in facilitating financial transactions for ransomware actors.[32] Analysis of SUEX's transactions revealed that over forty percent of its transactions were associated with illicit actors.[33] It thus follows, criminals must be deprived of their financial channels, or

26. *See America Is Being Held for Ransom. It Needs to Fight Back*, N.Y. TIMES (Sept. 20, 2021), https://www.nytimes.com/2021/09/20/opinion/ransomware-biden-russia.html [https://perma.cc/9P82-JFPR].

27. Victoria G. Myers, *Cybersecurity and Ag – 1, Cybercriminals Take Aim at America's Food Supply*, PROGRESSIVE FARMER (Sept. 21, 2021, 12:38 PM), https://www.dtnpf.com/agriculture/web/ag/news/business-inputs/article/2021/09/21/cybercriminals-take-aim-americas?referrer=twitter#.YUoitsVV5cM.twitter [https://perma.cc/UC8X-LH9X].

28. *See* PUBLIC SERVICE ANNOUNCEMENT, *supra* note 18.

29. John Reed Stark, *Ransomware's Dirty Little Secret: Most Corporate Victims Pay*, LAW360 (Feb. 6, 2019, 2:21 PM), https://www.johnreedstark.com/wp-content/uploads/sites/180/2019/02/Safari-Feb-6-2019-at-147-PM.pdf [https://perma.cc/UN6G-U5RF].

30. *Id.*

31. *Id.*

32. DEP'T OF THE TREASURY, UPDATED ADVISORY OF POTENTIAL SANCTIONS RISKS FOR FACILITATING RANSOMWARE PAYMENTS 3 (2021), https://home.treasury.gov/system/files/126/ofac_ransomware_advisory.pdf [https://perma.cc/KHG2-N774] [hereinafter UPDATED ADVISORY].

33. *Id.*

they will continue to flourish.[34]

III. NOT A NEW THREAT TO AGRICULTURE

Often overlooked in its significance, the United States agriculture industry accounts for almost 20 percent of the nation's economic activity.[35] Held under almost entirely private ownership, the industry is "composed of an estimated 2.1 million farms, 935,000 restaurants, and more than 200,000 registered food manufacturing, processing, and storage facilities."[36] In recent years, the industry has become more reliant on technology, utilizing "high-tech innovations like drones, GPS mapping, soil sensors and autonomous tractors, with vast data behind it all."[37] The same technology that has led to unprecedented expansion and innovation also exposes the agriculture industry to increased risk of cyberattacks, including ransomware.

A. The USDA's Vulnerabilities as a Federal Agency

In February of 2021, the USDA Office of Inspector General released an audit report on the USDA's security controls over the prevention and mitigation of ransomware within the Research, Education and Economics mission area.[38] The audit report indicated that the Research, Education, and Economics mission area of the USDA did not fully implement federally-mandated audit controls.[39] Although the full extent of the report was withheld from public release, it illustrates the USDA's awareness of critical weaknesses within the agency.[40]

34. Stark, *supra* note 29; *see also* ADVISORY ON POTENTIAL SANCTIONS, *supra* note 13, at 3.

35. *Food and Agriculture Sector*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY (Aug. 26, 2022, 4:28 PM), https://www.cisa.gov/food-and-agriculture-sector [https://perma.cc/94MZ-N4UK].

36. *Id.*

37. Ryan McCrimmon & Martin Matishak, *Cyberattack on Food Supply Followed Years of Warnings*, POLITICO (June 5, 2021, 12:04 PM), https://www.politico.com/news/2021/06/05/how-ransomware-hackers-came-for-americans-beef-491936 [https://perma.cc/PU54-5PQF]; see Ashley Ellixson et al., *Legal and Economic Implications of Farm Data: Ownership and Possible Protections*, 24 DRAKE J. AGRIC. L. 1, 52-53 (2019) ("[F]arm scale data . . . may include soil nutrient information, as-applied rates, and yield monitor data. Metadata may include the number of acres, and when, where, and which inputs were applied and cultivars planted.").

38. OFF. OF INSPECTOR GEN. U.S. DEP'T OF AGRIC., USDA'S SECURITY CONTROLS OVER THE PREVENTION AND MITIGATION OF RANSOMWARE 2 (2021), https://www.usda.gov/sites/default/files/audit-reports/50501-0024-12_FR_508_FOIA_redacted_public.pdf [https://perma.cc/35JD-C6GJ] [hereinafter USDA'S SECURITY CONTROLS].

39. *Id.*

40. *Id.*

Meanwhile, while other industries utilize information sharing and analysis centers (ISACs) to coordinate their responses to cyber threats, the USDA disbanded its group in 2008 due to "lack of activity and information flow."[41] Experts did not agree with this decision, which persists today, despite an increased risk of attack.[42]

The continued lack of cyber-security within the USDA was criticized by Congress in a 2019 Senate Staff Report.[43] In the 2019 Senate Staff Report, the subcommittee emphasized the criticality of the security holes identifying four significant problem areas.[44] First, the USDA stores sensitive private information, including employment records and social security information of American taxpayers.[45] Second, the USDA also maintains databases with market sensitive commodity information capable of causing serious economic harm.[46] Third, the USDA houses information pertaining to participation in the Select Agent Program, which identifies hazardous pathogens and toxins that "have the potential to pose a severe threat to human, animal, or plant health and safety, or to animal or plant products."[47] Lastly, the USDA houses the Food Safety Inspection Services' vulnerability assessments, which "inform the development of countermeasures to help prevent or mitigate the impacts of an intentional attack on the food supply."[48]

B. The Agriculture Industry as a Target

Agribusiness' are increasingly more vulnerable to the threat of ransomware attacks.[49] On September 1, 2021, the FBI's Cyber Division released a private industry notification warning of increased threats on the food and agriculture sector.[50] The notification warned of the negative impacts cyber-attacks have on the industry, including disrupting operations, financial loss, and negatively impacting

41. *Food Sector Abandons its ISAC*, ASIS ONLINE (Sept. 1, 2008), https://www.asisonline.org/security-management-magazine/articles/2008/09/food-sector-abandons-its-isac/ [https://perma.cc/9BLC-R2N8]; McCrimmon & Matishak, *supra* note 37.

42. *See generally Food Sector Abandons Its ISAC*, *supra* note 41.

43. *See generally* Staff of S. Subcomm. on Investigations, 116th Cong., Rep. on Federal Cybersecurity: America's Data at Risk 32-34 (Comm. Print 2019).

44. *See generally id.* at 66-72.

45. *Id.* at 66.

46. *Id.*

47. *Id.*

48. *Id.* at 67.

49. Ellixson et al., *supra* note 37, at 52 (explaining that aside from the value of raw data itself, agribusiness and technology firms have invested billions into "acquiring and developing farm data aggregation and analysis systems.").

50. *See* CYBER CRIMINAL ACTORS, *supra* note 3, at 1.

the food supply chain.[51] The FBI stressed larger organizations may be more attractive to criminals because the payout is potentially larger; nonetheless, smaller private operations should not dismiss the issue.[52] The industry notification came after months of ransomware attacks on agriculture and related industries.[53]

On May 30, 2021, REvil, a Russian-speaking group of cyber criminals, attacked JBS Foods, the second largest meat packer in the United States.[54] The attack disrupted meat production around the world, and it is estimated the halt in production reduced one quarter of the United States' meat processing capacity per day.[55] The aftershock caused a shortage in the United States' meat supply and drove up wholesale meat prices as much as 25%.[56] JBS paid an $11 million ransom to restore their data due to "the sophistication of the attack" even though the majority of JBS's plants remained operational.[57]

The JBS attack came less than a month after DarkSide, a Russian group, hacked the Colonial Pipeline and obtained access to computer networks through a single compromised password.[58] The pipeline experienced the hack on May 7, 2021 and paid a $4.4 million ransom the next day.[59] The news of the hack, however, was not without repercussion as areas in the southeastern United States saw gas price increases of up to 6.3% due to consumer panic.[60]

In mid-September, NEW Cooperative, the fifty-first largest farm cooperative

51. *Id.*

52. *See id.* at 2.

53. *See generally id.*

54. *REvil, A Notorious Ransomware Gang, Was Behind JBS Cyberattack, The FBI Says*, NPR (June 3, 2021, 8:17 AM ET), https://www.npr.org/2021/06/03/1002819883/revil-a-notorious-ransomware-gang-was-behind-jbs-cyberattack-the-fbi-says [https://perma.cc/E63D-B4ZN] [hereinafter *REvil*].

55. *Cybersecurity War: Lessons from the JBS Ransomware Attack*, BAROAN TECHS. (Aug. 26, 2022, 4:35 PM), https://www.baroan.com/understanding-jbs-ransomware-attack/ [https://perma.cc/WNM2-CGDQ].

56. CYBER CRIMINAL ACTORS, *supra* note 3, at 3.

57. *Meat Giant JBS Pays $11m in Ransom to Resolve Cyber-Attack*, BBC (June 10, 2021), https://www.bbc.com/news/business-57423008 [https://perma.cc/7N59-TXFQ] [hereinafter *JBS Pays $11m*].

58. Brian Fung & Geneva Sands, *Ransomware Attackers Used Compromised Password to Access Colonial Pipeline Network*, CNN POLITICS (June 4, 2021, 8:32 PM ET), https://www.cnn.com/2021/06/04/politics/colonial-pipeline-ransomware-attack-password/index.html [https://perma.cc/9MMW-ZJC3]; *see REvil*, *supra* note 53.

59. Fung & Sands, *supra* note 58.

60. *Effects of the Colonial Pipeline Hack on the Price of Gas*, THE COUNCIL FOR CMTY. & ECON. RSCH. (Aug. 26, 2022, 4:39 PM), https://www.coli.org/effects-of-the-colonial-pipeline-hack-on-the-price-of-gas/ [https://perma.cc/2GQH-DS55].

in the United States, confirmed a cybersecurity attack impacting some of the company's devices and systems.[61] According to Bloomberg, the cybercriminal group BlackMatter demanded a ransom payment of $5.9 million.[62] The attack came after President Biden warned Vladimir Putin "that Russia-based hacking groups should steer clear of [sixteen] critical sectors to the [United States'] economy."[63] The food and agriculture sector was included in President Biden's warning to the Russians.[64] However, the group defined "critical" as it saw fit and attacked the sector anyway.[65] Although NEW Cooperative is solely located in Iowa, the hack came at the beginning of harvest season with the cooperative being one of the largest crop buyers of its members.[66] According to Bloomberg, BlackMatter had stolen the cooperative's financial information, human resources data, research and development information, and source code for "SoilMap," a platform for agriculture producers.[67] BlackMatter threatened to publish the acquired data if the ransom was not paid.[68] As of October 2021, NEW Cooperative was back online at 50% automated capability.[69] However, the cooperative declined to comment as to whether it had paid BlackMatter's demand of $5.9 million.[70]

NEW Cooperative is not the first attack the agriculture industry has seen. Crystal Valley Cooperative based out of Mankato, Minnesota, fell victim to a cyber-attack just days following the NEW Cooperative attack.[71] The attack forced

61. Maggie Miller, *Major Agriculture Group New Cooperative Hit by Ransomware Attack*, THE HILL (Sept. 20, 2021, 5:26 PM ET), https://thehill.com/policy/cybersecurity/573082-agriculture-group-new-cooperative-hit-by-ransomware-attack [https://perma.cc/KEW5-6XSZ].

62. William Turton, *After Biden Warning, Hackers Define 'Critical' as They See Fit*, BLOOMBERG (Sept. 20, 2021, 7:42 PM), https://www.bloomberg.com/news/articles/2021-09-20/iowa-based-grain-cooperative-hit-with-ransomware-attack [https://perma.cc/KC56-224R].

63. *Id.*

64. *Id.*; *see Food and Agriculture Sector*, *supra* note 35.

65. Turton, *supra* note 62.

66. *Id.*

67. *Id.*

68. *See id.*

69. Donnelle Eller, *Iowa Grain Cooperative Says it's Working to Restore Automated Operations, But Remains Silent on Cyberattack Ransom*, DES MOINES REG. (Oct. 6, 2021, 8:24 AM CT), https://www.desmoinesregister.com/story/money/agriculture/2021/10/06/iowa-grain-cooperative-recovering-cyberattack-remains-mum-ransom/6007123001/ [https://perma.cc/DHD4-BUMM].

70. *Id.*

71. David Jones, *Ransomware Compromises Customer Data in Farm Co-op Attack*, CYBERSECURITY DIVE (Sept. 24, 2021), https://www.cybersecuritydive.com/news/agriculture-food-ransomware-coop/607080/ [https://perma.cc/9QME-9GXK].

the cooperative to rely on manual hand tickets during its busiest time of the year.[72] The cooperative warned members to monitor their bank and financial accounts following the exposure to unauthorized criminals.[73]

Just as the FBI had predicted, the agriculture sector took a big hit in 2021 with over 52 complaints.[74] The NEW Cooperative, Crystal Valley, JBS, and Colonial Pipeline attacks illustrate how serious the threat of ransomware is to our food system, agriculture, and economy. Major vulnerabilities exist in all tiers of the agricultural system. Without proper controls in place, continued attacks could expose large amounts of sensitive private information and shut down our markets and food system. The clock is ticking and every second the industry wastes, the greater the risk, and the larger the damage will be. It is not *if* the next attack occurs, it is *when.*

C. Precision Agriculture & Producer Level Vulnerabilities

The agriculture industry, like many other industries, has experienced substantial growth driven by technological innovation.[75] The goal and result of which has been increased production while utilizing less land and fewer resources.[76] The concept of precision agriculture is not new to the agriculture industry, but it has seen exponential innovation in the last few decades. First used in combines during the 1990s, precision agriculture is not one concept, but rather a toolbox that allows producers to be more efficient.[77] Three of the most influential precision agriculture tools are as follows: computer mapping of yield and soil data, allowing custom crop management within fields; guidance systems such as auto-steer, which reduce operator error by utilizing precise field locations; and variable rate technology, which enables customized seeding and application of fertilizer, chemicals, and pesticides from GPS controls in the cabs of tractors.[78] Although precision agriculture provides producers with increased efficiency and profitability, it also exposes producers to significant risk, especially if the proper data controls are not in place.

Even more troubling, agricultural data contains private, sensitive information of the entities and producers from which it derives. Data collected on the

72. *Id.*

73. *Id.*

74. INTERNET CRIME REPORT 2021, *supra* note 16, at 15 (In 2021, IC3 received 649 total complaints from organizations belonging to a critical infrastructure sector.).

75. Jody L. Ferris, Note, *Data Privacy and Protection in the Agriculture Industry: Is Federal Regulation Necessary?*, 18 MINN. J.L. SCI. & TECH. 309, 309 (2017).

76. *Id.*

77. DAVID SCHIMMELPFENNIG, U.S. DEP'T OF AGRIC. ECON. RSCH. SERV., FARM PROFITS AND ADOPTION OF PRECISION AGRICULTURE 1, 3 (2016), https://www.ers.usda.gov/webdocs/publications/80326/err-217.pdf?v=5045.5 [https://perma.cc/96VK-HRNN].

78. *Id.* at 3, 4.

producer level "has many characteristics which make it sensitive."[79] First, data may include personal private information of producers.[80] Information can include names, addresses, property locations, crop yield information, income, and farmland value.[81] Second, producer data is extremely sensitive due to its economic value.[82] Agricultural technology providers could use producer data to create new products.[83] Similarly, commodity traders may use the data to make trade decisions.[84]

Cybersecurity's threat is not a new one to the agriculture industry, and the government has known of the holes in data security for several years.[85] Although data protection law is one of the fastest growing areas of legal regulation, no current regulation is specifically tailored to the agriculture industry.[86] In 2015, the House Agriculture Committee conducted a hearing concerning private big data in the agriculture industry.[87] Data ownership and privacy were chief concerns, but most panelists ultimately agreed that little to no government intervention was needed.[88] Legal requirements for data privacy and security in agriculture are limited to generalized federal and state data privacy and data protection laws.[89] This includes the Gramm-Leach-Bliley Act for financial services and Federal Trade Commission (FTC) regulations.[90]

In 2016, the FBI published a report stating that the Food and Agriculture Sector "is increasingly vulnerable to cyberattacks as farmers become more reliant on digitized data."[91] While this farm-level data is useful to predict trends or make

79. Ferris, *supra* note 75, at 316.

80. *Id.*

81. *Id.*; see generally Ellixson et al., *supra* note 37, at 53 (explaining three categories of farm data "(1) data deliberately collected for the farm by the farm, (2) data collected by a second party at the request of the farmer, and (3) data collected about the farm by an outside party.").

82. *Id.* at 317.

83. *Id.*

84. *Id.*

85. *See id.* at 318.

86. *Id.*; *see* Ellixson et al., *supra* note 37, at 52 ("As of 2018, no existing laws address data ownership or implications of misappropriations of that data."). *But see id.* at 54-55 (Explaining section 1619 of the 2008 Farm Bill (7 U.S.C. §8791(b)(2) (2018)), disallowed the USDA and Farm Service Agency (FSA) from making geospatial data available to the public.).

87. MEGAN STUBBS, CONG. RES. SERV., R44331, BIG DATA IN U.S. AGRICULTURE 3 (2016).

88. *Id.*

89. Ferris, *supra* note 75, 318.

90. *Id.* at 319.

91. FED. BUREAU OF INVESTIGATION CYBER DIV., PIN NO. 160331-001, SMART FARMING

production practices more efficient, criminals could use this same data to exploit markets.[92] To the same effect, individual producers often do not have as broad of access to security practices that a large entity may have.[93] Although ransomware attackers typically target larger entities, a breach on smaller entities or individuals has the potential to be catastrophic. Agricultural data qualities and characteristics require greater protection than is currently provided.

IV. THE BIDEN ADMINISTRATION'S RESPONSE TO INCREASED CYBER SECURITY THREATS

On May 12, 2021, President Biden signed an Executive Order (the Order) to improve and protect the nation's cybersecurity and federal government networks.[94] Under the Order, President Biden encouraged private sector companies to follow the federal government's lead and "take ambitious measures to augment and align cybersecurity investments with the goal of minimizing future incidents."[95] Specifically, the Order will help remove barriers to threating information shared between the government and the private sector, modernize and implement stronger security standards in the federal government, improve software supply chain security, establish a cybersecurity safety review board, create a playbook for responding to cyber incidents, improve network detection of cybersecurity incidents on federal government networks, and improve investigative and remediation capabilities.[96] The President indicated that incremental improvements are not enough:

> The Federal Government needs to make bold changes and significant investments in order to defend the vital institutions that underpin the American way of life. The Federal Government must bring to bear the full scope of its authorities and resources to protect and secure its computer systems, whether

MAY INCREASE CYBER TARGETING AGAINST US FOOD AND AGRICULTURE SECTOR 1 (2016), https://info.publicintelligence.net/FBI-SmartFarmHacking.pdf [https://perma.cc/56TN-VKLP] (utilizing precision agriculture technology) [hereinafter SMART FARMING].

92. *Id.*

93. Rachel Schutte, *Why You Need Cybersecurity on the Farm*, AM. AGRICULTURIST (June 1, 2022), https://www.farmprogress.com/farm-business/why-you-need-cybersecurity-farm [https://perma.cc/U558-A7PJ].

94. *FACT SHEET: President Signs Executive Order Charting New Course to Improve the Nation's Cybersecurity and Protect Federal Government Networks*, WHITE HOUSE BRIEFING ROOM (May 12, 2021), https://www.whitehouse.gov/briefing-room/statements-releases/2021/05/12/fact-sheet-president-signs-executive-order-charting-new-course-to-improve-the-nations-cybersecurity-and-protect-federal-government-networks/ [https://perma.cc/QH9S-97QC] [hereinafter *FACT SHEET*].

95. *Id.*

96. *See generally id.*

> they are cloud-based, on-premises, or hybrid. The scope of protection and security must include systems that process data (information technology (IT)) and those that run the vital machinery that ensures our safety (operational technology (OT)).[97]

The President's firm stance on cybersecurity further indicates all federal agencies will have to meet or exceed the standards and requirements set forth in the Order.[98] This Order includes the USDA, which has for too long taken the reactive approach.

On November 3, 2021, the Cyber Security and Infrastructure Security Agency (CISA) released *Binding Operational Directive 22-01 - Reducing the Significant Risk of Known Exploited Vulnerabilities*.[99] Binding operational directives are "compulsory direction[s] to federal, executive branch, departments and agencies for purposes of safeguarding federal information and information systems."[100] The Department of Homeland Security (DHS) is authorized by federal law to develop and oversee the implementation of binding operation directives.[101] Federal agencies are required to comply with directives developed by the CISA, an operational component of DHS.[102] The directive required that within sixty days of issuance, agencies review and update internal vulnerability management procedures and, if requested, provide copies of these policies and procedures to the CISA.[103] Additionally, it required remediation of vulnerabilities in accordance with the CISA-managed vulnerability catalog and a report on the status of vulnerabilities.[104]

In accordance with Executive Order 14028, CISA released the *Federal Government Cybersecurity Incident and Vulnerability Response Playbooks* on November 16, 2021[105] As required by the Order, the playbooks serve the purpose of standardizing and improving the practices used by federal agencies to better "identify,

97. Exec. Order No. 14028, 86 Fed. Reg. 26633 (May 12, 2021).

98. *See generally id.*

99. *Binding Operational Directive 22-01 - Reducing the Significant Risk of Known Exploited Vulnerabilities*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY (Nov. 3, 2021), https://www.cisa.gov/binding-operational-directive-22-01 [https://perma.cc/T723-PUBD] [hereinafter *Binding Operational Directive*].

100. *Id.*

101. *Id.*; 44 U.S.C. § 3552 (2018).

102. *Binding Operational Directive*, *supra* note 99; § 3552.

103. *Binding Operational Directive*, *supra* note 99.

104. *Id.*

105. *CISA Releases Incident and Vulnerability Response Playbooks to Strengthen Cybersecurity for Federal Civilian Agencies*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY (Jan. 24, 2022), https://www.cisa.gov/news/2021/11/16/cisa-releases-incident-and-vulnerability-response-playbooks-strengthen [https://perma.cc/BMH4-CS6R].

remediate, and recover from vulnerabilities and incidents affecting their systems."[106] The playbook includes both an *Incident Response Playbook*, providing a standardized response process for cybersecurity incidents, and a *Vulnerability Response Playbook*, providing a straightforward and effective means for an organization to prioritize responses by focusing on vulnerabilities already being actively exploited.[107] Both playbooks apply to all Federal Civilian Executive Branch (FCEB) agencies, which are information systems operated by or used by the agency, and contractors or other organizations on behalf of an agency.[108]

President Biden's Order, paired with CISA's binding directive and the Response Playbooks, indicate the federal government's recognition of the seriousness of the risk that ransomware presents. The USDA, as a federal agency, is required to comply with the guidelines directed to all FCEB's.[109] Compliance with these authorities will be a stark contrast to the USDA's history of reactive approaches and lax cybersecurity policies.[110] It is crucial the USDA and other pertinent agencies comply with the federally mandated requirements to protect the United States' security, economy, and food supply.

V. REMAINING GAPS IN THE REGULATORY LANDSCAPE

If the agriculture industry is essential to the nation's economy and food supply, why then is the industry largely unprepared for a ransomware attack? The private industry cannot effectively combat ransomware attacks on its own. To properly protect such a vital industry, action must be taken in both the public and private sectors. Private industry leaders are voicing the need for more regulation and enforcement of existing statutory authority.[111] Following the Colonial Pipeline attack, CEO Joseph Blount urged for government action, pleading "[u]ltimately

106. *Id.*

107. *Id.*

108. CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, CYBERSECURITY INCIDENT & VULNERABILITY RESPONSE PLAYBOOKS, OPERATIONAL PROCEDURES FOR PLANNING AND CONDUCTING CYBERSECURITY INCIDENT AND VULNERABILITY RESPONSE ACTIVITIES IN FCEB INFORMATION SYSTEMS 3, 21 (2021), https://www.cisa.gov/sites/default/files/publications/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf [https://perma.cc/84FF-4XK8] [hereinafter CYBERSECURITY INCIDENT]; *see Binding Operational Directive*, *supra* note 99 (the USDA falls under the authority of CISA).

109. CYBERSECURITY INCIDENT, *supra* note 108, at 25.

110. *See* USDA's SECURITY CONTROLS, *supra* note 38, at 2; *see also* Staff of S. Comm. on Investigations, 116th Cong., Rep. on Federal Cybersecurity: America's Data at Risk (Comm. Print 2019).

111. *See e.g.*, William Turton & Kartikay Mehrotra, *Hackers Breached Colonial Pipeline Using Compromised Password*, BLOOMBERG (June 4, 2021, 7:58 PM), https://www.bloomberglaw.com/ms/product/blaw/document/QU6WS5T0G1NA [https://perma.cc/5HAB-GHVL].

the government needs to focus on the actors themselves. As a private company, we don't have a political capability of shutting down the host countries that have these bad actors in them."[112] Intervention should not stop at targeting the actors themselves. Further, although the agriculture industry is financially supported by the federal government via the Farm Bill and other means, no agriculture-specific legislation exists to safeguard the security of critical agricultural data.[113] Lastly, the USDA must, as a governmental agency, increase safeguards to comply with President Biden's Order and at least meet minimum security requirements.[114]

A. Shut Down Illicit Actors Through Enforcement of Already Enacted Federal Statutes

Although ransomware payments may violate Office of Foreign Assets Control (OFAC) regulations, Trading with the Enemy Act (TWEA), Bank Secrecy Act (BSA), and Anti-Money Laundering Act (AML), strict enforcement is necessary to deter persons from paying ransoms.[115] Specific legislation pertaining to ransomware and other cyber-attacks might make standards and enforcement actions clearer. On August 5, 2021, the Sanction and Stop Ransomware Act of 2021 was introduced by Senator Marco Rubio (R-FL) to the Senate.[116] This Bill would set cybersecurity standards for critical infrastructure, regulation for cryptocurrency exchange, established reporting requirements, and imposed sanctions under OFAC.[117] The Bill has yet to move to a vote.[118] Other bills, such as H.R. 3138, State and Local Cyber Security and Improvement Act, and Senate Resolution 410, supporting a national cybersecurity awareness month, provide hope for increased awareness and enforcement against ransomware.[119]

112. *Id.* (concerning hackers who have found a safe haven in Russia).

113. *See generally* WHAT IS THE FARM BILL?, *supra* note 5; *but see* Ferris, *supra* note 75, at 319.

114. *See generally* Exec. Order No. 14028, 86 Fed. Reg. 26633 (2021) (e.g., sharing of threat and incident information, updating cyber security protections, implementing cloud security, etc.).

115. *See infra* Section VI., Subsection B.

116. Sanction and Stop Ransomware Act of 2021, S. 2666, 117th Cong. (2021).

117. S. 2666, at § 4(d).

118. S. 2666.

119. State and Local Cyber Security Improvement Act, H.R. 3138, 117th Cong. (2021); Cyber Security Awareness Month, S. Res. 410, 117th Cong. (2021).

B. Develop Mandatory, Agriculture-Specific Data Security Regulations

The next key step in protecting the agriculture sector is developing mandatory, agriculture-specific data security regulations. "The agriculture industry is increasingly one of the most concentrated industries," with consolidation observed in almost every area.[120] This oligopolistic structure is the perfect storm for a ransomware attack, which could lead to the exposure of millions of producers. The key players in the agriculture sector must be held accountable for the protection of the sensitive producer data they harbor.

Experts have discussed whether agriculture-specific data privacy regulations would be beneficial to the industry, citing to the Agriculture Data Act of 2018.[121] This Bill, unfortunately, never became law, but it did receive bipartisan support and was helpful in outlining the need for agriculture-specific data privacy legislation.[122] Enacting similar legislation to the 2018 Act would "have significant impacts on establishing federal [agriculture data] standards."[123] It would create recognized standards for security and data privacy, regulations related to third party use, anonymization, and demonstrate a commitment to increasing the effectiveness and evaluation of government programs.[124] Industry-specific data protection is seemingly one of the most straight-forward ways to set minimum security and anonymity standards that would protect sensitive producer and market information.[125] While it "is not the typical type of personal, identifiable data protected under federal privacy laws, protection [of agricultural data] remains warranted."[126] Reidentification techniques utilized by cyber criminals may allow more data to be identifiable than previously realized.[127] Mandatory agriculture-specific legislation is therefore essential to the integrity of our agriculture system and protection against cyberattacks.

C. Hold the USDA Accountable

Just as federal regulations must be enforced to be effective, the same can be said with regard to executive orders. As stated previously, President Biden's Order provided that the head of each agency shall update existing plans to prioritize the

120. Jennifer Zwagerman, *Agriculture & Data Privacy: I Want a HIPPA(POTAMUS) for Christmas. . .Maybe*, 8 TEX. A&M L. REV. 685, 694 (2021) (areas include food processing, manufacturing, meat packing, grain processing, and input supplies of seed and chemicals).

121. *Id.* at 721; *See* Agriculture Data Act of 2018, S. 2487, 115th Cong. (2018).

122. Zwagerman, *supra* note 120, at 725.

123. *Id.*

124. *Id.*

125. *Id.* at 731.

126. *Id.*

127. *Id.*; *see also* Ferris, *supra* note 75, at 318.

adoption and use of cloud technology, develop a "Zero Trust" architecture, and provide a report to the director of the Office of Management and Budget (OMB) and Assistant to the President and National Security Advisor within sixty days of the issuance of the Order.[128] Zero Trust architecture mandates deployment of multifactor authentication and encryption of data.[129] As agencies continue to adopt cloud technology, they are required to do so in a way that allows the federal government to have oversight to "prevent, detect, assess, and remediate cyber incidents."[130] Under the Order, the USDA, along with other administrative agencies, must implement the federal government's playbook to "ensure all Federal agencies meet a certain threshold and are prepared to take uniform steps to identify and mitigate a threat."[131] Compliance to the Order is a critical step in ensuring the safety of critical infrastructure that directly and indirectly impacts our food system.

VI. PRIVATE ACTION WILL AGGREGATE

The White House acknowledged that federal action alone will not be enough to protect our infrastructure from cyber incidents.[132] The private industry must make their own determinations in cyber security improvement, but the industry is encouraged to follow the federal government's lead, including referencing the playbook.[133] If there are network vulnerabilities in the food and agriculture sector, criminal actors will continue to torment stakeholders, regardless of their size.[134] While larger entities are often more attractive due to their capabilities to pay out large sums of ransom, significant risks exist for smaller entities or agriculture producers.[135] Regardless of size, there are general best practices stakeholders can implement to mitigate their risk of intrusion.

A. Strengthen Passwords & Utilize Multi-Factor Authentication

Although government action will arguably bring more widespread protection from cyberattacks, private action should not be overlooked in terms of its value. First and foremost, producers and other private agriculture actors should utilize strong passwords and regularly change their passwords.[136] In the recent attack on NEW Cooperative, researchers indicated that the same password, "chicken1" was

128. Exec. Order No. 14028, 86 Fed. Reg. 26633 (May 17, 2021).
129. *FACT SHEET*, *supra* note 94.
130. 86 Fed. Reg. 26633.
131. *FACT SHEET*, *supra* note 94.
132. *Id.*
133. *Id.*
134. CYBER CRIMINAL ACTORS, *supra* note 3, at 5.
135. *Id.* at 2.
136. *Id.* at 4.

common among the company's employees and was used *over ten times*.[137] The same issue resulted in the attack on the Colonial Pipeline where one leaked password, along with lack of Multi-Factor Authentication (MFA), resulted in shutdown of the pipeline and fuel shortages across the East Coast.[138] Ideally, passwords should be greater than seven characters, with nine to ten being preferred; a password of ten characters can take 3,000 years to hack while a seven character one can take as little as a day.[139] Capitalizing the first letter or varying letters, inserting numbers randomly into or at the end of words, and utilizing special characters can further complicate the ability to hack a password.[140]

Although the use of sophisticated passwords helps mitigate risk, they are by themselves often insufficient to protect against a breach.[141] Single authentication, or the use of only a password to authenticate access, is the weakest level of authentication and exposes a person or organization to an increased risk of unauthorized access.[142] Instead, MFA should be utilized "to provide a higher level of safety and facilitate continuous protection."[143] In fact, according to a report by Microsoft, over 99.9% of breached systems did not use MFA.[144] One of the most utilized MFA tools is the mobile MFA application.[145] The applications allow a user to log in and then prompt the user to input a one time code.[146]

There are many MFA applications to choose from, but a 2021 study from the University of Denver analyzed the effectiveness of ten different applications.[147] Among those studied, Microsoft, SecureAuth, and Symantec ranked among the

137. Jonathan Greig, *After Ransomware Attack, Company Finds 650+ Breached Credentials from NEW Cooperative Employees*, ZD NET (Sept. 21, 2021), https://www.zdnet.com/article/after-ransomware-attack-company-finds-650-breached-credentials-from-new-cooperative-ceo-employees/ [https://perma.cc/C82Z-XCRT] (emphasis added).

138. Turton & Mehrotra, *supra* note 111.

139. Yash Tiwari, *How Easy is it for a Hacker to Crack Your Password?*, INFOSEC (Feb. 1, 2017), https://resources.infosecinstitute.com/topic/easy-hacker-crack-password/ [https://perma.cc/8ZJZ-UQNS].

140. *Id.*

141. *See* Aleksandr Ometov et al., *Multi-Factor Authentication: A Survey*, 2 (1) CRYPTOGRAPHY, Jan. 5, 2018, at 1, 1.

142. *Id.* at 2.

143. *Id.*

144. Kevin Jensen et al., UNIV. OF DENVER, MULTI-FACTOR AUTHENTICATION APPLICATION ASSESSMENT: RISK ASSESSMENT OF EXPERT-RECOMMENDED MFA MOBILE APPLICATIONS 1 (2021), https://wayworkshop.org/2021/papers/way2021-jensen.pdf [https://perma.cc/8JLX-SXM8].

145. *Id.*

146. *Id.*

147. *Id.*

most secure and effective.[148] Nevertheless, the use of a MFA method provides increased security from cyber threats.[149] Pairing a strong password with MFA provides the best protection from cyberattacks and other security breaches.

B. Should a Ransom Be Paid? Important Legal Considerations if Considering Making a Ransomware Payment

In the case of an attack, the private sector should not pay a ransom for two specific reasons. First, malicious actors seek a ransom because there is a market for ransomware payments.[150] Removing the supply to this market will disincentivize such actors from maliciously receiving payment. Second, paying a ransom further exposes a person to liability.[151] Ransom payment does not guarantee the return of useable data nor does it guarantee return of any stolen data.[152] Furthermore, by paying a ransom, a person subjects themself to potential regulatory or statutory liability.[153]

Nevertheless, many corporate victims choose to pay ransom requested by illicit individuals. Companies may choose to do this for a variety of reasons, but it is important to realize payments do not make the issue disappear, even if a company's data is restored. Ransom payments have the potential to make a company more likely to fall victim to another attack because cyber criminals know the victim will pay. Nevertheless, when a victim is considering paying a ransom there are important legal considerations that must be evaluated. Ransom payments enable criminals and adversaries with a sanction nexus to profit and advance their illicit aims, including funding activities adverse to United States national security and foreign policy objectives.[154] Although penalties in this area are nothing new, the advisories published by FinCEN and OFAC likely signal a shift in increased oversight of ransomware payments.[155]

148. *Id.* at 5 (Table 2).

149. *See id.* at 1.

150. *See* INTERNET CRIME REPORT 2020, *supra* note 2, at 14.

151. *See id.* (not only may a person lose the ransom they paid, but they may also lose their data regardless of having paid such ransom); *see also* ADVISORY ON POTENTIAL SANCTIONS, *supra* note 13, at 3 ("OFAC may impose civil penalties for sanctions violations based on strict liability").

152. *See* INTERNET CRIME REPORT 2020, *supra* note 2, at 14.

153. *See* Trading with the Enemy Act, 50 U.S.C §§ 4301–4341 (2018); International Emergency Economic Powers Act, 50 U.S.C § 1705 (2018); *see also* ADVISORY ON POTENTIAL SANCTIONS, *supra* note 13, at 3.

154. ADVISORY ON POTENTIAL SANCTIONS, *supra* note 13, at 3.

155. Colin Jennings, et al., *4 Compliance Tips Amid Increased Ransomware Scrutiny*, LAW 360 (Oct. 8, 2020, 4:55 PM), https://www.law360.com/articles/1317078

1. Ransomware Payments Enable Criminal Activity, Threaten United States National Security Interests, and May Violate OFAC Regulations

On September 21, 2021, OFAC issued an updated advisory highlighting the sanctions risk associated with ransomware payments.[156] The advisory highlighted the demand for payments has increased during the COVID-19 pandemic when many people were working remotely.[157] The advisory further indicated that OFAC strongly discourages ransomware payments by issuing the following statement: "[t]he U.S. government strongly discourages all private companies and citizens from paying ransom or extortion demands and recommends focusing on strengthening defensive and resilience measures to prevent and protect against ransomware attacks."[158] Further, the advisory emphasized that ransomware may enable criminal activity, threaten United States national security interests, and violate OFAC regulations.[159]

General supply and demand theory applies to the payment of ransom to cyber criminals; the more victims who pay the request create an increased incentive to continue to terrorize institutions.[160] Payments not only enable cyber criminals to make a profit, but payments may also advance illicit aims.[161] For example, "ransomware payments made to sanctioned persons or to comprehensively sanctioned jurisdictions could be used to fund activities adverse to the national security and foreign policy objectives of the United States."[162] Moreover, there is no evidence to suggest payment of a ransom will guarantee return of data or prevent future attacks from occurring.[163]

Further, "facilitating ransomware payments on behalf of a victim may violate OFAC regulations."[164] Under the authority of the International Emergency Economic Powers Act (IEEPA) or the TWEA, United States persons are prohibited from engaging in transactions, directly or indirectly, with individuals on OFAC's Specially Designated Nationals and Blocked Persons list (SDN List), other

[https://perma.cc/84DZ-Y8DS]; *see also* John Reed Stark, *An OFAC Compliance Checklist for Ransomware Payments*, LAW360 (Feb. 2, 2021, 5:43 PM), https://www.law360.com/articles/1349647/an-ofac-compliance-checklist-for-ransomware-payments [https://perma.cc/X4TQ-HUTW].

156. *See* ADVISORY ON POTENTIAL SANCTIONS, *supra* note 13, at 1.
157. *Id.*
158. *Id.*
159. *Id.* at 3.
160. *Id.*
161. *Id.*
162. *Id.*
163. *Id.*
164. DEP'T OF THE TREASURY, *supra* note 32, at 1.

blocked persons, or those covered by country or regional embargoes.[165] Moreover, OFAC may impose civil penalties for sanction violations based on strict liability.[166] Therefore, persons subject to United States jurisdiction may be held civilly liable "*even if such person did not know or have reason to know*" they were engaging in a transaction that is prohibited under OFAC's law and regulations.[167] This includes the payment of ransom in the case of a ransomware attack.[168]

2. Ransomware Attacks may Impose Liability Under the Bank Secrecy Act, and Anti-money Laundering Laws

Agricultural organizations in the banking and finances industries are exposed to even greater liability if they facilitate cyber ransom payments. Banks, virtual security exchangers, and other financial institutions face obligations under the BSA and the AML.[169] These obligations include preventing institutions from being used to advance criminal activity and filing Suspicious Activity Reports (SARs) on suspect actions occurring through financial institutions.[170] Similarly, criminal money laundering laws, such as the AML prohibit conducting transactions with the proceeds of criminal activity.[171] Application of the BSA and AML have even been extended to individuals making peer-to-peer exchanges of convertible virtual currency.[172]

Facilitating ransom payments has significant policy, statutory, and regulatory implications. The BSA and AML's enforcement against companies and individual persons further illustrates the breadth of their application. Thus, paired with

165. *Id.*; *see* Trading with the Enemy Act, 50 U.S.C §§ 4301–4341 (2018); International Emergency Economic Powers Act, 50 U.S.C §§ 1701–1706 (2018).

166. DEP'T OF THE TREASURY, *supra* note 32, at 4; §§ 4301-4341; §§ 1701-1706.

167. DEP'T OF THE TREASURY, *supra* note 32, at 4 (emphasis added).

168. *See id.*; *see also* §§ 4301–4341; §§ 1701–06.

169. Paul Rosen & Carlton Green, *Ransomware: What Every Corporate Executive Needs to Know*, CORP. COUNS. 2 (Oct. 30, 2017), https://www.law.com/corpcounsel/sites/corpcounsel/2017/10/30/ransomware-what-every-corporate-executive-needs-to-know/?slreturn=20210917171632 [https://perma.cc/5BKR-KLUY]; *see also* 31 U.S.C. § 5311 (2018).

170. Rosen & Green, *supra* note 169, at 2.

171. *Id.*

172. *FinCEN Penalizes Peer-to Peer Virtual Currency Exchanger for Violations of Anti-Money Laundering Laws*, U.S. TREASURY FIN. CRIMES ENF'T NETWORK (Apr. 18, 2019), https://www.fincen.gov/news/news-releases/fincen-penalizes-peer-peer-virtual-currency-exchanger-violations-anti-money [https://perma.cc/4UTL-T97P] [hereinafter *FinCEN Penalizes*].

regulators' intent to crack down on ransomware payments, it would not be advisable to pay a ransom in the case of a cyberattack.[173]

C. Individuals or Organizations Should Plan for an Attack and Know How to Respond if One Occurs

Considering the increased frequency of cyberattacks, the best thing an individual or organization can do is develop a plan. Ideally, planning will enable a more efficient response and decrease liability or harm to the individual or organization.[174] To minimize the risk of violating United States sanction laws and the effect of a ransomware attack, companies should implement what is commonly referred to as an "action plan" or compliance program. Recommended actions for an appropriate risk-based compliance program are updated and secured backups, performance of due diligence, and notify and cooperate with law enforcement.[175]

The first recommendation is to update and secure backups.[176] Updated and secured backups allow leverage to be taken away from cyber criminals in the case of a ransomware attack because they will have nothing to "hold for ransom."[177] To ensure adequate security, backups should be kept separately from networks and be either offline or through a separate cloud-based service.[178] Organizations should regularly test their backups by recording the time it takes to restore systems vital to operations and documenting any difficulties encountered during the process.[179]

Although ransomware payments are not recommended, they may seem like the only option in instances such as backup failure or an illicit actor's threat of publishing sensitive information on the internet. Before initiating a ransomware payment, the victim, and any third-party advisors (such as insurance companies)

173. *See* U.S. TREASURY, ADVISORY ON RANSOMWARE AND THE USE OF THE FINANCIAL SYSTEM TO FACILITATE RANSOM PAYMENTS 4 (2020), https://www.fincen.gov/sites/default/files/advisory/2020-10-01/Advisory%20Ransomware%20FINAL%20508.pdf [https://perma.cc/7MB7-J3NZ] [hereinafter ADVISORY ON RANSOMWARE]; *see also FinCEN Penalizes*, *supra* note 171.

174. *See* Peter W. Baldwin et al., *Ransomware Payments May Violate Sanctions Laws, U.S. Treasury Department Warns*, FAEGRE DRINKER (Oct. 6, 2020), https://www.faegredrinker.com/en/insights/publications/2020/10/ransomware-payments-may-violate-sanctions-laws-us-treasury-department-warns [https://perma.cc/2FJ3-XDPK]; *see also* Stark, *supra* note 154.

175. Baldwin et al., *supra* note 174.

176. *Id.*

177. *See id*.

178. *Id.*

179. *Id.*

should conduct reasonable due diligence.[180] Any due diligence should be thoroughly documented.[181] Reasonable due diligence includes searching OFAC's SDN list and determining if attackers are from embargoed jurisdictions.[182]

Lastly, looping in law enforcement is an essential element of responding to a ransomware attack. Not only does notification allow the FBI to gather intelligence, but it may also enable greater protection from civil penalties if a ransom is paid to an illicit actor.[183] OFAC views a victim's prior cooperation with law enforcement to be a significant mitigating factor.[184] If an individual suspects they have fallen victim to a ransomware attack, it is recommended they contact OFAC and their local FBI field office or alert the FBI through the IC3.[185]

Developing and implementing a risk-based compliance program is crucial to being prepared for and responding efficiently to a ransomware attack. While the recommendations listed in this section are not exhaustive, they are a helpful foundation for mitigating risk associated with modern business.[186] Additional considerations include implementing training for staff according to their risk exposure level, building a ransomware-specific response team, employing ransomware experts as needed, and maintaining thorough documentation trail.[187] Unfortunately, "[n]o matter how sophisticated and vigilant, no company can ever enjoy immunity from a cyber-attack."[188] Sadly, until the United States government takes dramatic action, ransomware attacks will continue to occur and become more sophisticated and costly for victims.[189]

VII. CONCLUSION

Ransomware can no longer be ignored. With every attack, cybercriminals gain institutional knowledge and the power to increase the sophistication of the next attack.[190] By leaving the agriculture sector and its stakeholders exposed to this risk, we are essentially laying billions of dollars on the table, free for the taking.

180. *Id.*

181. *See id.*; Stark, *supra* note 155.

182. Baldwin et al., *supra* note 174.

183. *Id.*

184. ADVISORY ON POTENTIAL SANCTIONS, *supra* note 13, at 4.

185. *Id.*; Baldwin et al., *supra* note 173 (victims should be prepared to provide an overview of the attack, any identifying information of the attackers, and details concerning the ransom demand).

186. *See generally* Stark, *supra* note 155.

187. *Id.*

188. *Id.*

189. *Id.*

190. *Id.*

The JBS attack halted meat processing around the world and reduced the United States' capacity to 25%.[191] That was only one key event. Imagine if, instead, illicit actors attacked the USDA or multiple suppliers. We cannot continue to ignore the urgency of this issue.

To best combat ransomware, we need government intervention and private action. Without federal action, large private companies are likely to keep facilitating ransom payments by means of cyber insurance.[192] This means criminals will continue to be encouraged by the steady availability of "business." Similarly, private individuals or organizations, no matter their size, can make several changes to significantly reduce the risk of attack, including multifactor authorization, password changes, and introducing compliance controls.[193]

Federal action is necessary. Key federal statutes and regulations, such as OFAC, TWEA, BSA, and the AML, must be enforced for immediate effect. Enforcement will deter payments of ransom and help discourage ransomware attacks by exhausting the source.[194] The time has come for agriculture-specific data security regulations. The oligopolistic nature of the agriculture industry exposes it to greater risk of industry-wide harm and makes mass amounts of sensitive private information vulnerable. Lastly, it is essential the USDA steps up to the plate and complies with President Biden's Executive Order by implementing, at the very least, the minimal level of security and controls. It is simply unacceptable an agency of the federal government does not meet or exceed federally set requirements, especially for an industry essential to the nation's economy and food supply.

Private action, although seemingly smaller in scale, will aggregate and generate substantial effects.[195] Individuals and organizations can mitigate the risks of ransomware in three ways: strengthening passwords, not paying a ransom, and planning for an attack by testing backups, preparing due diligence, and implementing compliance programs.[196] Together these actions will decrease the damage incurred by individuals and organizations.[197] As a result, cyber-criminals will be deterred from implementing attacks.[198]

191. *JBS Pays $11m*, *supra* note 55; *see also* CYBER CRIMINAL ACTORS, *supra* note 3, at 3.

192. *See* Stark, *supra* note 155.

193. *Id.*

194. *See* ADVISORY ON RANSOMWARE, *supra* note 173, at 3.

195. *See generally* Stark, *supra* note 155.

196. *Id.*

197. *See id.*

198. *Id.*

Illustrated eloquently by the Farm Bill, the agriculture sector contributes significantly to this nation's economy and food supply, making it one of the most important industries in the United States.[199] We cannot leave such a vital industry unprotected any longer. Doing so could have disastrous consequences for our national security, economy, and food supply.

199. *See generally* WHAT IS THE FARM BILL?, *supra* note 5.