"Too small to be targeted:" Perceived Cybersecurity Vulnerabilities of Small-Scale U.S. Farmers

Lulu Rodriguez, Iowa State University
Kristine Micheletti, Iowa State University
Shuyang Qu, Iowa State University
Fally Masambuka-Kanchewa, Iowa State University

As agriculture becomes increasingly digitalized, farms face rising exposure to cyberthreats that jeopardize data security, productivity, and business continuity. This study examined small-scale crop and livestock producers' perceptions of cybersecurity risks, their experiences with cyberattacks, and their information sources across 12 U.S. Midwest states. Guided by the Social Amplification of Risk Framework (SARF), a mixed-mode survey design was used, combining online and mail questionnaires distributed to 14,000 small farms between November 2023 and April 2024. Findings revealed that while most farmers were moderately familiar with cybersecurity concepts and recognized the importance of protective action, many underestimated their likelihood of being targeted. Farmers expressed the greatest concern over personal identity theft and computer viruses but were less aware of broader operational vulnerabilities. The majority practiced basic protective behaviors such as anti-malware installation and data backup, yet fewer implemented advanced measures like encryption or multifactor authentication. Media, friends, and relatives were the most frequently cited information sources, while formal channels such as Extension services were seldom used. Results underscore a critical need for cybersecurity literacy programs tailored to rural communities and smallholder operations. The study extends SARF by showing how interpersonal communication and perceived relevance shape risk awareness and protective behavior in the agricultural sector. The insights also hold international value, offering a model for strengthening digital resilience in global farming systems.

Keywords: Cybersecurity in agriculture; cyber threats in farming; smallholder farmers' perceived cyber vulnerabilities; cybersecurity protective behaviors of small-scale farmers; farmers' cybersecurity information sources

Funding Source: Cybersecurity for Smart Agriculture, Presidential Interdisciplinary Research Initiative, Iowa State University

Introduction

Farming today is increasingly data-driven (MarketsandMarkets, 2024). Remote-controlled tractors, Global Positioning System (GPS)-enabled planting systems, and internet-connected sensors in animal sheds are now commonplace, bringing new levels of efficiency and precision to agricultural operations (Geil et al., 2018; Masere & Worth, 2015). However, this digital transformation has also opened the door to sophisticated cyberthreats—such as phishing emails, ransomware, and data breaches—that can cripple a farm's operations (Fagan, 2022).

The agricultural sector is not immune to cybersecurity threats. While large corporate farms are more visible targets for cybercriminals, small and midsize operations that have embraced digital technologies are equally vulnerable (Paez, 2021). Lacking the resources necessary to safeguard their systems (Alahmadi et al., 2022), small farms are often unable to absorb the financial losses resulting from cyberattacks (National Cybersecurity Alliance [NCA], 2022). They can also serve as "weak links that enable unauthorized access to larger networks" (NCA, 2022, p. 5). Understanding small farm operators' knowledge and awareness of cybersecurity risks is therefore critical for establishing protective measures, ensuring business continuity, and building resilience in an increasingly connected agricultural landscape.

Disruptions to the small farm networks that underpin the Midwest agricultural system could have far-reaching impacts, as the region is a major agricultural powerhouse often referred to as "America's breadbasket" (Climate Hubs, n.d.). Cyberattacks threaten not only people but also animals and crops. Many systems—such as automated ventilation and feeding mechanisms—are critical to farm operations and depend on uninterrupted electricity, water, and network connectivity (Nikander et al., 2020). Interruptions to these systems can endanger animal welfare and crop production. As global food security increasingly relies on interconnected digital networks, protecting even the smallest nodes within these systems—the small farms—is essential to ensuring the stability of agricultural supply chains worldwide. Attacks on poultry facilities, for instance, could result in the loss of thousands of birds, while cyber incidents targeting greenhouse systems could lead to devastating crop and revenue losses (Yazdinejad et al., 2020). Understanding producers' perceptions of cybersecurity threats is therefore vital for developing recommendations that strengthen the protection of farming systems and mitigate the impacts of cyber incidents on the broader agricultural sector.

This study aims to provide insights for those responsible for enhancing agricultural cybersecurity within the United States and beyond. As farms worldwide adopt increasingly digitized systems—such as precision agriculture, remote monitoring, and data-driven management—the vulnerabilities identified among small-scale U.S. farmers are likely mirrored in similar contexts elsewhere. This study examines the gap between technological adoption and cybersecurity preparedness, particularly among small and resource-constrained operations.

By identifying specific perceptions, knowledge gaps, and information-seeking behaviors, this research contributes to the design of more effective risk communication strategies and cybersecurity training programs that can be adapted for rural and smallholder farming communities globally. Its broader significance lies in advancing the growing body of knowledge on agricultural cybersecurity and providing a model for assessing vulnerabilities and strengthening digital resilience in farming systems.

Literature Review and Theoretical Framework

Through internet connectivity, digitalization has become one of the most transformative aspects of technological advancement in agriculture, enabling improvements in productivity and farming processes (Bush et al., 2025; Nikander et al., 2020). Technologies applied to agricultural production—such as soil moisture sensors, remote monitoring and control of livestock facilities, software-connected tractor implements, and precision agriculture systems—can optimize production conditions, increase resource efficiency, reduce waste, and improve both field management and food quality (Angyalos et al., 2021; Masere & Worth, 2015).

However, the adoption of these advanced technologies and farm information management systems has introduced new vulnerabilities into an industry that was previously largely mechanical. Their use has created an unsupervised network of information exchanged among producers, suppliers, vendors, and consumers, heightening susceptibility to cyberattacks that hackers can exploit to disrupt production (Drape et al., 2021; Duncan et al., 2019). Agriculture is now more vulnerable than ever to phishing campaigns containing malicious links and attachments, ransomware attacks leading to business disruptions and revenue loss, exposure of confidential data, and even intentional data falsification that can undermine system integrity (Barreto & Amaral, 2018).

Cybersecurity threats in agriculture manifest in diverse ways. According to the Federal Bureau of Investigation (FBI), criminals are expanding their activities, attacking a wider array of targets, threatening data or algorithms in livestock or equine management software, and compromising data used in water supply systems (FBI, 2021; Kulkarni et al., 2024). In general, farm staff are not trained to be cybersecurity experts (Angyalos et al., 2021). Their limited knowledge and resources exacerbate these risks (Sontowski et al., 2020; Moonsammy & Moonsammy, 2020). Smallholder farms are thus considered "soft targets" (FBI, 2021, p. 2)—relatively unprotected entities that rely primarily on basic prevention measures such as firewalls and endpoint protection platforms.

U.S. farm surveys have begun to document farmers' growing concerns. A Farm Bureau study conducted in 2014 found that 87% of farmer-respondents lacked a contingency plan to manage security breaches (Paez, 2021). Despite recognizing the value of computer security technologies, many were not comfortable adopting such systems (Duncan et al., 2019). As of 2020, fewer than 20% of farm operators surveyed in a *Farm Journal* Pulse poll reported confidence in their data security (Eckelkamp, 2020).

How might risk perception be amplified to enhance the adoption of protective measures? The Social Amplification of Risk Framework (SARF) provides a useful lens for examining public perceptions, values, and behaviors to explain how risk is perceived and communicated in society (Kasperson et al., 2022). SARF posits that risk perception is not determined solely by technical assessments of probability or severity but is shaped by how information about risk is transmitted, filtered, and amplified through social networks, institutions, and media (Kasperson et al., 2022). In the context of this study, the "risk" in question—cybersecurity threats to small-scale farm operations—is complex, largely invisible, and technical in nature, making it highly susceptible to processes of amplification and attenuation as it circulates through farmers' social environments.

SARF suggests that the way an issue is conveyed by various sources interacts with

psychological, social, and cultural processes in ways that may attenuate or amplify perceptions of risk and, in turn, shape protective attitudes and behaviors. Risk assessment involves subjective judgment, which helps explain why people respond differently to the hazards they perceive (Ali et al., 2020; Slovic et al., 1981).

According to SARF, individuals use a range of inferential rules or heuristics—such as perceived severity, familiarity, and controllability of a risk—rather than rely solely on statistical probabilities when assessing risks in everyday life (Jenkins et al., 2024; Slovic et al., 1981). Applied to cybersecurity in agriculture, these perceptions help explain how and why smallholder farmers view digital threats as they do. Because cyberthreats do not involve physical harm or visible damage, they may evoke weaker emotional responses compared to other agricultural risks. Unlike familiar farm hazards such as machinery injuries or animal disease outbreaks, cybersecurity risks lack direct sensory cues. Farmers who have never personally experienced a cyber threat incident may find it difficult to imagine or recognize it. Cyber risks may also be perceived as distant rather than immediate, delaying action and reducing perceived urgency—even though a single breach can lead to severe economic and operational disruptions. Taken together, these characteristics place farm cybersecurity risks in the "unknown" and "low dread" quadrant of the psychometric risk space (Slovic et al., 1986). This may help explain why smallholder farmers often underestimate the seriousness of digital vulnerabilities despite their increasing reliance on interconnected systems.

Purpose and Objectives

This study examines small-scale producers' perceptions of cybersecurity risks in the American heartland. Specifically, the objectives of this study are to:

1. Assess the level of cybersecurity awareness of small-scale crop and animal farmers, as well as their experience with cyberattacks.
2. Examine farmers' perceived vulnerabilities related to cybersecurity and identify the protective practices farmers have implemented against cyberthreats.
3. Determine farmers' primary sources of information about cybersecurity.

Methods

To investigate the perceptions, experiences, and behaviors of small-scale farmers in the U.S. Midwest related to cybersecurity threats, we conducted a quantitative survey, utilizing a mixed-mode strategy that combined online and mail-based data collection to reach a broader range of respondents (Dillman, 2011). This strategy was designed to overcome known barriers to digital engagement in rural communities and to enhance the representativeness of the sample. We began by distributing an invitation letter containing a QR code that linked to the online questionnaire. This letter was mailed to 14,000 small-scale farming and ranching operations across 12 Midwest states, namely Illinois, Indiana, Iowa, Kansas, Michigan, Minnesota, Missouri, Nebraska, North Dakota, Ohio, South Dakota, and Wisconsin. Following the designation set by the U.S. Department of Agriculture's National Institute of Food and Agriculture (n.d.), we defined "small-scale farms" as those with a gross cash farm income of $250,000 or less. Dynata, a market research company, recruited the respondents and provided the physical address of these farms and their operators.

The initial online outreach yielded 127 responses. To supplement this and increase

participation, we followed up by mailing paper versions of the questionnaire to 5,000 randomly selected addresses from the original list that had not responded. This second wave generated an additional 215 completed surveys. In total, the combined response yielded 342 completed questionnaires between November 22, 2023 and April 31, 2024, resulting in an overall response rate of 2.4%. After data cleaning to remove incomplete or duplicate entries, 278 usable responses remained for analysis.

The low response rate (2.4%) despite the mixed-mode survey sampling strategy likely resulted from a combination of seasonal timing and digital access barriers. The questionnaire was distributed during the harvest season**,** when farmers are typically busiest and have little time nor interest in completing surveys, especially those not directly linked to immediate farm benefits. The initial online invitation with the QR code also may have limited accessibility. Many expressed not being comfortable using QR codes to participate in online surveys; others reported limited internet connectivity.

It is important to consider the implications of this low level of participation on the precision and representativeness of the results. According to sample size calculations by Kosar et al. (2018), a sample of 278 yields a margin of error of approximately ±6% at a 95% confidence level. Because an ideal margin of error is generally below 5% (Bartlett et al., 2001; Kosar et al., 2018), the generalizability of the findings is somewhat constrained. This limitation should be considered when interpreting and applying the results.

The survey instrument was structured based on the study's objectives and was composed of five parts: (1) *Awareness of cybersecurity* was assessed through five-point Likert scale items (1=not at all familiar; 5=extremely familiar) evaluating respondents' self-reported understanding of the terms "cybersecurity," "cyberattack," and "cyberthreats." (2) *Experience with cyberattacks* was gauged through yes/no/unsure questions about the nature and frequency of any cybersecurity breaches encountered (Have you encountered cyberattack incidents before? Have you ever suspected that you have been a victim of a cyberattack?). (3) *Perceptions of cybersecurity risk* ($\alpha = .86$) were measured using a four-item five-point Likert scale (1=strongly disagree; 5=strongly agree) assessing respondents' concern about cyberattacks and perceived vulnerability (I am concerned about my farm's data system being cyberattacked; My farm is likely a target of cyberattacks; My farm is susceptible to cyberattacks; If it happens, a cyberattack will have a significant impact on my farm). (4) *Specific cybersecurity concerns* ($\alpha = .90$) were ascertained by making respondents rate the extent to which they were likely to experience the following scenarios on a five-point Likert scale (1=not likely at all; 5=extremely likely): My computer system becoming corrupted by a virus; My computer being taken over by a hacker; My files becoming corrupted by a computer virus; My personal identity being stolen (e.g., credit cards, social security number); My agribusiness or farm identity being stolen (e.g., through loan fraud); My personal identity being stolen (e.g., thefts of credit cards, social security number); and My computer becoming infected with a virus by visiting a website. (5) *Information sources* were determined through multiple choice and ranked preference items identifying where farmers typically learn about cybersecurity issues and the information sources they were likely to use to learn about protective practices (other farmers, friends, conventional media, online sources, social media, Extension agents, local libraries, government agencies). Two other sections asked about farming and demographic characteristics.

No previously validated instruments were found that adequately capture the specific

experiences and management contexts of small-scale Midwestern farmers; thus, we developed questionnaire items tailored to this population. Item wording was informed by a review of relevant literature and refined through expert feedback and pilot testing to ensure content validity and clarity.

Prior to data collection, the questionnaire was reviewed by a panel of experts in agricultural communication, extension education, and risk perception to ensure both content and face validity. Feedback from this panel helped refine question clarity, relevance, and structure, ensuring alignment with both the theoretical framework (SARF) and the practical realities of small-scale farming. Cronbach's alphas for the two constructs—perceived risks of cyberattacks on their farm operation and farmers' level of concerns—were computed to measure internal consistency and reliability of scale items. The scales measuring the two concepts were deemed reliable ($\alpha_{risks} = .86$, and $\alpha_{concerns} = .90$).

Descriptive statistical analyses (using means, frequencies, and percentages) were conducted using SPSS to summarize the data. These analyses allowed us to describe the respondents' perceived risks, level of familiarity with cybersecurity concepts, personal experience with attacks, and trusted sources of information.

Results

We surveyed 278 farmers across 12 Midwestern states to assess their perceptions of cybersecurity threats, their demographic and farming characteristics, personal experiences with cyberattacks, protective practices, and preferred sources of information. Conducted between November 2023 and April 2024, the study presents a revealing picture of a sector navigating the intersection of tradition and technology.

Demographic Characteristics

Most respondents identified as male (83.7%, *n* = 220). Participants ranged in age from 28 to 89 years, with the largest proportion falling within the 66–70 age group (20.6%, *n* = 53), followed by those aged 71–75 (15.8%, *n* = 40) and 61–65 (14.2%, *n* = 36). About one-third of respondents (32.8%, *n* = 86) reported holding a bachelor's degree, while only 0.8% (*n* = 2) had completed some high school or less (Table 1).

Table 1

Demographic Characteristics of Respondents

Demographic Characteristic	*Count*	*Valid %*
Age Brackets (*n* = 253)		
28-30	2	0.8
31-35	6	2.4
36-40	10	4.0

Demographic Characteristic	*Count*	*Valid %*
41-45	13	5.1
46-50	12	4.7
50-55	16	6.3
56-60	25	9.8
61-65	36	14.2
66-70	52	20.6
71-75	40	15.8
76-80	23	9.1
81-85	13	5.1
86-90	5	2.0
Sex (n = 263)		
Male	220	79.1
Female	40	14.4
Do not want to answer	3	1.1
Education (n = 262)		
Some high school or less	2	0.8
High school graduate or GED	49	18.7
Some college, no degree	46	17.6
Two-year associate degree	39	14.9
Bachelor's degree	86	32.8
Graduate or professional degree	40	15.3

Farming Characteristics

Respondents reported owning and/or managing multiple types of farm operations. Most

grew row crops (80.9%, *n* = 225), about half raised livestock (51.1%, *n* = 142), and a smaller number were engaged in seed production (7.2%, *n* = 20). In addition to corn and soybeans, other crops they produced included alfalfa, sweet corn, winter wheat, small grains, fruits, vegetables, hay, specialty crops, native grasses, trees, and riparian buffers. Livestock operations consisted primarily of dairy and equine enterprises.

Farm operations were distributed across 12 states: Iowa (25.7%, *n* = 69), Wisconsin (13.0%, *n* = 35), Nebraska (11.2%, *n* = 30), Minnesota (10.0%, *n* = 27), Illinois (8.9%, *n* = 24), Ohio (6.3%, *n* = 17), Michigan (5.9%, *n* = 16), Kansas (5.6%, *n* = 15), Missouri (4.8%, *n* = 13), Indiana (4.1%, *n* = 11), South Dakota (2.6%, *n* = 7), and North Dakota (1.9%, *n* = 5).

Farmers were asked which internet-connected technologies they used in daily operations. Among crop producers, yield monitoring systems (60.4%, *n* = 168) and sprayers or fertilizer applicators (60.1%, *n* = 167) were most common, while in-field sensors were least used (14.0%, *n* = 39). Among livestock operators, electronic identification (EID) technologies were most prevalent (11.9%, *n* = 33), followed by automated weighing systems (6.8%, *n* = 19). Proxy technologies for measuring methane emissions were rare (0.7%, *n* = 2) (Table 2).

Awareness of and Experience with Cyberattacks

We assessed the extent to which farmer respondents considered themselves familiar with the terms "cybersecurity," "*cyberattack*," and "cyberthreat." Among those who answered this question (*n* = 273), most reported some level of familiarity: 13.9% (*n* = 38) were slightly familiar, 21.2% (*n* = 58) somewhat familiar, 46.5% (*n* = 127) moderately familiar, and 15.8% (*n* = 43 extremely familiar. Only 2.6% (*n* = 7) indicated they were not at all familiar with the terms.

Respondents were also asked whether they had personally experienced a cyberattack. Over half (59.3%, *n* = 160) reported no prior encounters, while 23.0% (*n* = 62) said they had experienced a cyberattack. Another 17.8% (*n* = 48) were unsure whether they had been targeted.

Table 2

Farming Characteristics of Respondents

Farming Characteristic	*Count*	*Valid %*
Farming operation (*n* = 278)[1]		
Row crops	225	80.9
Livestock	142	51.1
Seed production	20	7.2
Other	33	11.9
Farm location (*n* = 269)		
Iowa	69	25.7
Wisconsin	35	13.0
Nebraska	30	11.2
Minnesota	27	10.0
Illinois	24	8.9
Ohio	17	6.3
Michigan	16	5.9
Kansas	15	5.6

Farming Characteristic	*Count*	*Valid %*
Missouri	13	4.8
Indiana	11	4.1
South Dakota	7	2.6
North Dakota	5	1.9
Technologies connected to the internet[1]		
Crop: Yield monitoring	168	60.4
Crop: Sprayers and fertilizer applicators	167	60.1
Crop: Automatic steering	153	55.0
Crop: Section and row control on planters	136	48.9
Crop: Variable rate input application	115	41.4
Crop: Spatial data management systems	43	15.5
Crop: In-field electronic sensors	39	14.0
Livestock: Electronic identification (EID) solutions	33	11.9
Other	26	9.4
Livestock: Automated weighing systems	19	6.8
Livestock: Low-cost feed and water intake recording	17	6.1
Livestock: Animal sensing systems	13	4.7
Livestock: Imaging solutions	9	3.2
Livestock: GPS-tracking for extensive systems	8	2.9
Livestock: Application of advanced data analytics to big data	8	2.9
Livestock: Proxy technologies for measuring methane emissions	2	0.7

[1]Percentages don't add to 100% because respondents were able to select more than one response.

Perceived Risk of Cyberattacks

Producers also rated their level of concern about cyberattacks on a five-point Likert scale ranging from "strongly disagree" to "strongly agree." Nearly half (46.8%, $n = 127$) were moderately to strongly worried that their farm data systems could be hacked, and 36.7% ($n = 99$) believed their operations were vulnerable to cyberattacks. Similarly, 46.6% ($n = 126$) agreed that a cyberattack would have a significant impact on their farms. Despite these concerns, 45.1% ($n = 122$) disagreed that their farms were likely targets, while 38.7% ($n = 105$) were unsure (neither agree nor disagree) (Table 3).

Table 3

Farmers' Level of Concern about Cyberattacks

	I am concerned about my farm's data system being cyberattacked.		My farm is likely a target of cyberattacks.		My farm is susceptible to cyberattacks.		If it happens, a cyberattack will have a significant impact on my farm.	
	Count	*Valid %*	*Count*	*Valid %*	*Count*	*Valid %*	*Count*	*Valid %*
Strongly disagree	24	8.9	37	13.7	27	10.0	25	9.3
Moderately disagree	51	18.8	85	31.4	58	21.5	48	17.8
Neither disagree nor agree	69	25.5	105	38.7	86	31.9	71	26.3
Moderately agree	89	32.8	36	13.3	79	29.3	90	33.3
Strongly agree	38	14.0	8	3.0	20	7.4	36	13.3
Total	271	100.0	271	100.0	270	100.0	270	100.0

Protection Behaviors

Respondents reported their engagement in various cybersecurity practices (n = 265). The most common was installing anti-malware software (79.2%, n = 210), followed by backing up essential files (66.4%, n = 176), keeping software updated (57.7%, n = 153), and using high-entropy passwords (55.5%, n = 147). Multi-factor authentication was used by 45.3% (n = 120), indicating moderate adoption of more advanced security measures. In contrast, few respondents reported implementing physical access controls (17.4%, n = 46), encrypting sensitive files (6.0%, n = 16), or employing other unspecified practices (6.8%, n = 18). Notably, 7.9% (n = 21) indicated they did not practice any of the listed cybersecurity behaviors.

Sources of Information about Cybersecurity Threats

We asked where farmers obtained information about cybersecurity. A large majority (84.3%, n = 214) learned about the topic through the media, while 34.3% (n = 87) said they became aware through friends or relatives who had experienced cybercrimes. Among those inclined to seek additional information, over half (53.1%, n = 130) said they would consult personal networks (friends and family), followed by online sources (42.4%, n = 104) and conventional mass media (39.6%, n = 97).

Conclusions, Recommendations and Implications

The adoption of agricultural technology brings an increased risk of cybersecurity attacks on farms and agribusinesses, potentially destabilizing food supply chains and harming communities and the broader economy. These systems are susceptible to hackers who can exploit

vulnerabilities to disrupt production and confuse those downstream who depend on the supply chain.

Our findings suggest that producers are conceptually aware that cybersecurity is an important issue and that network disruptions may hinder farm operations. However, although they recognize the existence of cyberthreats and the value of protective measures, many do not consider themselves likely targets of external attacks and therefore have not implemented adequate safeguards against online threats. This disconnect underscores a dangerous blind spot: while small-scale farmers acknowledge their growing vulnerability to cyberattacks, many believe they are too small to be targeted and consequently forgo cyber protection measures. The findings align with previous research (e.g., Yazdinejad, 2021) indicating that although farmers have embraced advanced technologies, many have not kept pace with the cybersecurity measures required to protect these systems.

Overconfidence and limited access to objective information may cause individuals to underestimate potential dangers, consistent with Jenkins et al.'s (2024) findings on the psychological landscape of risk perception. However, risks exist simply by virtue of being connected to the internet. This finding thus serves as a wake-up call: although large corporate farms may appear to be the primary targets of cyberattacks, small operations are equally—if not more—vulnerable because of their limited resources and often outdated security systems.

We also found a promising level of awareness and implementation of basic cybersecurity practices—such as anti-malware installation, data backup, and regular software updates—among Midwest farmers. Nevertheless, the relatively low adoption of more advanced or institutional-level measures, such as encryption and physical access controls, reveals gaps that could leave systems vulnerable to breaches, particularly in shared environments. This finding underscores the importance of continued education and support to promote the adoption of multifactor authentication and encryption practices, which are increasingly essential as digital threats evolve. The fact that nearly 8% of respondents reported taking no protective measures highlights the need for targeted outreach to engage this segment and promote cybersecurity as a shared responsibility. Overall, these results point to the importance of pairing comprehensive cybersecurity practices with knowledge about basic digital hygiene.

Respondents reported being most concerned about stolen identities and computer viruses—individual-level issues that overlook the interconnectedness of networks within the bioeconomy. Family farms differ from their corporate counterparts in that they often use home computers for both personal and business purposes (Duncan et al., 2019), thereby increasing their risk of cyberattacks. A network breach might begin with the cracking of a Wi-Fi password at the farm level, allowing intruders to obtain credentials through rogue access points, trick users into reinstalling keys already in use, decrypt packets transmitted via Wi-Fi–enabled devices, fake gateway addresses to collect information, or redirect traffic to fraudulent websites. Such incidents at the small-farm level can serve as entry points for cybercriminals into larger agricultural networks, making small farms weak links in a much broader chain. A cybersecurity threat at any stage of the food and agricultural system—from production to consumer purchase—can place the entire system at risk.

The concerns reported by respondents could serve as starting points for communication campaigns on cybersecurity responsibilities, available resources, and management tools. Communication efforts should prioritize digital literacy and cyber hygiene training to help

farmers navigate privacy settings, identify and avoid phishing attempts, and use technology safely and responsibly. In short, mitigation strategies should emphasize the rationale for investing in cybersecurity. Future studies could examine the effectiveness of communication strategies in increasing farmers' willingness to attend cybersecurity training and adopt protective behaviors.

Our findings also show that friends and family members were the most frequently cited information sources among those seeking guidance on protective behaviors. Online sources followed closely, while conventional mass media such as radio, television, and newspapers were used less often. Fewer respondents relied on formal or institutional sources, such as Extension agents, farmer organizations, or government agencies. Universities and social media channels were used intermittently. Overall, the data suggest a strong reliance on interpersonal and digital sources over institutional or traditional media channels. This raises questions about the accuracy of information being shared. Relying on family and peers is a double-edged sword—while these sources are often considered trustworthy, they may not always provide accurate or up-to-date information.

These findings have important implications for the design of communication strategies and the dissemination of outreach and educational materials. The strong reliance on friends, family, and online sources underscores the importance of informal networks and digital access in shaping knowledge and decision-making. Efforts to distribute accurate and timely information should therefore leverage trusted community influencers and improve the credibility of online content. The relatively low use of institutional sources, such as government agencies, universities, and Extension services, suggests potential issues of trust, accessibility, or perceived relevance for smallholder farmers in the Midwest. Additionally, the limited role of libraries and formal farmer organizations implies that traditional information infrastructure may be underutilized or inadequately supported. To maximize impact, communication efforts should integrate interpersonal and digital approaches while strengthening institutional channels to rebuild trust and reach broader audiences effectively.

The results highlight the need for improved digital literacy training and cybersecurity outreach tailored to rural communities. Suggested strategies include workshops, farm-level risk management toolkits, and messaging that presents the business case for cybersecurity investments. The study also found that few farmers have established response plans for cyber incidents or recognize the risks associated with corrupted data. The FBI (2021) recommends several "low-hanging fruit" actions to mitigate cyberthreats, such as implementing a recovery plan that involves regular data backups; maintaining multiple copies of data in physically separate, segmented, and secure locations (e.g., hard drives or cloud storage); using multifactor authentication and strong passwords; and installing and regularly updating antivirus and anti-malware software.

This study contributes to the Social Amplification of Risk Framework (SARF) by applying it to a new and underexplored context—cybersecurity risks in agriculture—and demonstrating how farmers' perceptions, experiences, and information networks shape their understanding and response to digital threats. In this study, SARF provided a useful lens for examining how small-scale farmers interpret cybersecurity threats that are often invisible, technical, and abstract. The findings show that while farmers recognize the general importance of cybersecurity, many do not perceive their own farms as likely targets, indicating a risk attenuation effect. Although many were aware of cybersecurity issues, they tended to downplay

their personal susceptibility, assuming that attacks are more likely to target large corporate farms.

At the same time, the study reveals that information about cyber risks spreads primarily through interpersonal and mass media channels rather than formal Extension systems. This pattern suggests that risk signals are often filtered and reshaped through trusted personal networks. When trusted peers minimize the threat, concern tends to diminish, which helps explain why awareness does not always translate into protective action.

The findings underscore the need for targeted risk communication strategies that amplify accurate risk signals, correct misconceptions, and make abstract technological risks personally relevant to farmers. Such interventions should aim to strengthen accurate perceptions, reduce complacency, and encourage proactive digital protection behaviors. Thus, this study not only operationalizes SARF in a novel agricultural context but also offers insights that refine its utility for understanding how emerging, technology-driven risks are socially constructed and managed in rural settings.

This research is also relevant to the practice of international agricultural and extension education, as it highlights the growing importance of digital literacy and cybersecurity awareness as integral components of modern agricultural extension. As farming systems worldwide become increasingly dependent on digital technologies, extension professionals are being called upon not only to promote innovations in production and sustainability but also to safeguard the technological infrastructure that supports them. The findings reveal that even among technologically progressive farmers, significant gaps remain in understanding and managing cyber risks—gaps that extension educators are uniquely positioned to address. Integrating cybersecurity into agricultural education and extension programming can equip farmers with the knowledge and skills to protect sensitive data, maintain business continuity, and build resilience against digital threats.

The study provides evidence that can guide global extension systems—particularly in developing regions where smallholders are rapidly adopting digital tools—on how to tailor cybersecurity education to local contexts, information networks, and cultural norms. In doing so, it advances the broader mission of empowering farmers with the competencies needed to thrive safely and sustainably in an increasingly digital agricultural landscape.

The study provides evidence that can guide global extension systems—particularly in developing regions where smallholders are rapidly adopting digital tools—on how to tailor cybersecurity education to local contexts, information networks, and cultural norms. In doing so, it advances the broader mission of empowering farmers with the competencies needed to thrive safely and sustainably in an increasingly digital agricultural landscape.

Limitations

Our low response rate limits the generalizability of the findings. Although a mixed-mode survey strategy was used to increase participation, only a small proportion of the 14,000 farmers contacted ultimately completed the questionnaire. A response rate of this magnitude increases the likelihood of nonresponse bias, meaning that those who chose to participate may differ systematically from those who did not. For example, respondents may have been more technologically engaged, more concerned about cybersecurity, or simply more available during

the data collection period than the broader population of small-scale Midwest farmers. As a result, the sample may not fully represent the diversity of views, experiences, or digital capacities present across the region. Because generalizability depends on whether the sample reflects the characteristics of the target population, the low response rate constrains the extent to which the results can be confidently applied to all small-scale farms in the Midwest or beyond.

The study also relied on newly developed questionnaire items rather than previously validated scales. Although this approach enhanced the contextual relevance of the measures to small-scale Midwestern farming operations, it may limit the comparability of these findings with prior research.

References

Alahmadi, A. N., Rehman, S. U., Alhazmi, H. S., Glynn, D. G., Shoaib, H., & Solé, P. (2022). Cyber-security threats and side-channel attacks for digital agriculture. *Sensors*, *22*(9), 3520. https://doi.org/10.3390/s22093520

Ali, M., Man, N., & Muharam, F. M. (2020). Intention level of farmers to use information communication technologies for agricultural risk management in Malaysia. *Journal of International Agricultural and Extension Education, 27*(2), 108-117. https://doi.org/10.5191/jiaee.2020.272108

Angyalos, Z., Botos, S., & Szilágyi, R. (2021). The importance of cybersecurity in modern agriculture. *Journal of Agricultural Informatics, 12*(2), 1-8. https://doi.org/10.17700/jai.2021.12.2.604

Barreto, L., & Amaral, A. (2018, September). Smart farming: Cyber security challenges. In *2018 International Conference on Intelligent Systems (IS)* (pp. 870-876). IEEE. https://doi.org/10.1109/IS.2018.8710531

Bartlett, J. E., II, Kotrlik, J. W. K. J. W., & Higgins, C. C. H. C. C. (2001). Organizational research: Determining appropriate sample size in survey research. *Information Technology, Learning, and Performance Journal*, *19*(1), 43.

Bush, S. A., Baker, C. N., Bunch, J., Baker, L., Loizzo, J. L., & Myers, B. (2025). Big data: Usage and application of big data in the human dimensions of agricultural and natural resources (ANR). *Journal of International Agricultural and Extension Education, 32*(1). https://doi.org/10.4148/2831-5960.1501

Climate Hubs. (n.d.). *Agriculture in the Midwest.* U.S. Department of Agriculture. https://www.climatehubs.usda.gov/hubs/midwest/topic/agriculture-midwest

Dillman, D. A. (2011). *Mail and internet surveys: The tailored design method—2007 update with new internet, visual, and mixed-mode guide*. John Wiley & Sons.

Drape, T., Magerkorth, N., Sen, A., Simpson, J., Seibel, M., Murch, R. S., & Duncan, S. E. (2021). Assessing the role of cyberbiosecurity in agriculture: A case study. *Frontiers in Bioengineering and Biotechnology, 9*(737927). https://doi.org/10.3389/fbioe.2021.737927

Duncan, S. E., Reinhard, R., Williams, R. C., Ramsey, F., Thomason, W., Lee, K., Dudek, N., Mostaghimi, S., Colbert, E., & Murch, R. (2019). Cyberbiosecurity: A new perspective on protecting U.S. food and agricultural system. *Frontiers in Bioengineering and*

Biotechnology, *7*(63), 1-7. https://doi.org/10.3389/fbioe.2019.00063

Eckelkamp, M. (2020, March 9). *FJ Pulse: Less than 20% of farmers confident in their data security.* Scoop. https://www.thedailyscoop.com/news/new-products/fj-pulse-less-20-farmers-confident-their-data-security

Fagan, C. F. (2022). *Critical vulnerabilities in the U.S. food sector and the next crippling attack.* Homeland Security Today. https://www.hstoday.us/featured/critical-vulnerabilities-in-the-u-s-food-sector-and-the-next-crippling-attack/

Federal Bureau of Investigation. (2021). *Cyber criminal actors targeting the food and agriculture sector with ransomware attack —Private Industry Notification.* FBI-CISA. https://www.cisa.gov/sites/default/files/publications/PIN_20210901.pdf

Food and Agriculture Organization. (2009). *Global agriculture towards 2050. How to feed the world 2050—High-level expert forum.* FAO. https://www.fao.org/fileadmin/templates/wsfs/docs/Issues_papers/HLEF2050_Global_Agriculture.pdf

Geil, A., Sagers, G., Spaulding, A. D., & Wolf, J. R. (2018). Cybersecurity on the farm: An assessment of cyber security practices in the United States agriculture industry. *International Food and Agribusiness Management Review, 21*(3), 317-334. https://doi.org/10.22434/IFAMR2017.0045

Jenkins, S. C., Lachlan, R. F., & Osman, M. (2024). An integrative framework for mapping the psychological landscape of risk perception. *Scientific Reports*, *14*¸10989. https://doi.org/10.1038/s41598-024-59189-y

Kasperson, R. E., Webler, T., Ram, B., & Sutton, J. (2022). The social amplification of risk framework: New perspectives. *Risk Analysis, 42*(7), 1367-1380. http://dx.doi.org/10.1111/risa.13926

Kosar, T., Bohra, S., & Mernik, M. (2018). A systematic mapping study driven by the margin of error. *Journal of Systems and Software*, *144*, 439-449. http://dx.doi.org/10.1016/j.jss.2018.06.078

Kulkarni, A., Wang, Y., Gopinath, M., Sobien, D., Rahman, A., & Batarseh, F. A. (2024). A review of cybersecurity incidents in the food and agriculture sector. ArXiv Cryptography and Security. https://doi.org/10.48550/arXiv.2403.08036

MarketsandMarkets. (2024). *Agriculture IoT market by hardware, application, farm size, production stage, and geography.* MarketsandMarkets. https://www.marketsandmarkets.com/Market-Reports/iot-in-agriculture-market-199564903.html?gclid=EAIaIQobChMI9MThusv79gIVg_TjBx0zNwxXEAAYAyAAEgI 85PD_BwE

Masere, T. P., & Worth, S. (2015). Applicability of APSIM in decision-making by small-scale resource-constrained farmers: The case of Lower Gweru Communal Area, Zimbabwe. *Journal of International Agricultural and Extension Education, 22*(3), 20-34. https://doi.org/10.5191/jiaee.2015.22302

Moonsammy, S., & Moonsammy, D. M. (2020). Social media application in agriculture

Extension programming for small scale rural farmers: Is knowledge impeding the lack of adoption? *Journal of International Agricultural and Extension Education, 27*(3), 27-42. https://doi.org/10.5191/jiaee.2020.27327

National Cybersecurity Alliance. (2022). *National Cybersecurity Alliance statement regarding incorrect small business statistics.* NCA. https://staysafeonline.org/news-press/press-release/national-cyber-security-alliance-statement-regarding-incorrect-small-business-statistic/

National Institute of Food and Agriculture. (n.d.). *Small and family farms.* U.S. Department of Agriculture. https://www.nifa.usda.gov/topics/small-family-farms#:~:text=Farming%20and%20Ranching,-Agricultural%20Safety&text=More%20than%2090%20percent%20of,income%20of%20%2425 0%2C000%2C%20or%20less

Nikander, J., Manninen, O., & Laajalahti, M. (2020). Requirements for cybersecurity in agricultural communication networks. *Computers and Electronics in Agriculture, 179*¸105776. https://doi.org/10.1016/j.compag.2020.105776

Paez, M. (2021, March 10). *Client advisory: Dealing with increasing cyber risks in agriculture.* MarshMcLennan. https://www.marshmma.com/us/insights/details/client-advisory-dealing-with-increasing-cyber-risks-in-agriculture.html

Slovic, P., Fischhoff, B., & Lichtenstein, S. (1981). Perceived risk: Psychological factors and social implications. In *Proceedings of the Royal Society A, 376*(1764), 17-34. https://doi.org/10.1098/rspa.1981.0073

Slovic, P., Fischhoff, B., & Lichtenstein, S. (1986). The psychometric study of risk perception. In V. T. Covello, J. Menkes & J. Mumpower (Eds.), *Risk evaluation and. management—Contemporary issues in risk analysis* (Vol. 1, pp. 3-24). Springer. https://doi.org/10.1007/978-1-4613-2103-3_1

Sontowski, S., Gupta, M., Chukkapalli, S. S. L., Abdelsalam, M., Mittal, S., Joshi, A., & Sandhu, R. (2020). Cyber attacks on smart farming infrastructure. In *Proceedings of the 2020 IEEE 6th International Conference on Collaboration and Internet Computing* (pp. 135-144). https://doi.org/10.1109/CIC50333.2020.00025

Yazdinejad, A., Zolfaghari, B., Azmoodeh, A., Dehghantanha, A., Karimipour, H., Fraser, E., Green, A. G., Russell, C., & Duncan, E. (2021). A review on security of smart farming and precision agriculture: Security aspects, attacks, threats and countermeasures. *Applied Sciences, 11*, 7518. https://doi.org/10.3390/app11167518