frontiers | Frontiers in Sustainable Food Systems

POLICY AND PRACTICE REVIEWS
published: 21 June 2022
doi: 10.3389/fsufs.2022.884187

On-Farm Data Security: Practical Recommendations for Securing Farm Data

Mehdi Hazrati, Rozita Dara and Jasmin Kaur*

School of Computer Science, University of Guelph, Guelph, ON, Canada

The growth in the use of Information and Communications Technology (ICT) and Artificial intelligence (AI) has improved the productivity and efficiency of modern agriculture, which is commonly referred to as precision farming. Precision farming solutions are dependent on collecting a large amount of data from farms. Despite the many advantages of precision farming, security threats are a major challenge that is continuously on the rise and can harm various stakeholders in the agricultural system. These security issues may result in security breaches that could lead to unauthorized access to farmers' confidential data, identity theft, reputation loss, financial loss, or disruption to the food supply chain. Security breaches can occur because of an intentional or unintentional actions or incidents. Research suggests that humans play a key role in causing security breaches due to errors or system vulnerabilities. Farming is no different from other sectors. There is a growing need to protect data and IT assets on farms by raising awareness, promoting security best practices and standards, and embedding security practices into the systems. This paper provides recommendations for farmers on how they can mitigate potential security threats in precision farming. These recommendations are categorized into human-centric solutions, technology-based solutions, and physical aspect solutions. The paper also provides recommendations for Agriculture Technology Providers (ATPs) on best practices that can mitigate security risks.

Keywords: information security, security breach, digital agriculture, farming, security standards, securing farms, Agriculture Technology Providers

OPEN ACCESS

Edited by:
Shambhu J. Upadhyaya,
University at Buffalo, United States

Reviewed by:
Ting Xie,
University at Buffalo, United States
Sumita Mishra,
Rochester Institute of Technology, United States
George Lawrence Sanders,
University at Buffalo, United States

****Correspondence:***
Rozita Dara
drozita@uoguelph.ca

Specialty section:
This article was submitted to Climate-Smart Food Systems, a section of the journal Frontiers in Sustainable Food Systems

Received: *21 March 2022*
Accepted: *26 May 2022*
Published: *21 June 2022*

Citation:
Hazrati M, Dara R and Kaur J (2022) On-Farm Data Security: Practical Recommendations for Securing Farm Data. Front. Sustain. Food Syst. 6:884187. doi: 10.3389/fsufs.2022.884187

INTRODUCTION

With the advancement of Artificial Intelligence (AI) and Internet of Things (IoT), the use of precision agriculture has been exponentially increasing. According to the MarketsandMarkets report (MarketsandMarkets, 2022), $8.5 billion USD was the precision farming market in 2022 and is expected to grow to 15.6 billion by 2030. Precision farming uses technological innovations in data collection and processing to enhance farm production and raising livestock. Precision agriculture has enabled farmers to make more informed decisions about farm production and use of resources. For example, with the help of precision agriculture technologies, farmers can monitor the crop status by observing and measuring variables such as soil condition, irrigation, fertilizer and pesticide effect, plant health, and crop yield. Similarly, the farmers can monitor the health of livestock animals by recording their food and water intake, weight, behavior, temperature, respiration rate, and sounds produced by animals.

These technologies are highly dependent on processing large volumes of data collected from farms (Cisternas et al., 2020). The data are collected using smart sensors, agricultural drones, and other farm technologies. According to IBM, 500,000 data points were being generated on an average farm per day in 2019 (IBM, 2021). This size is expected to grow to 4 million by 2036. The collected data helps gain insights into farm management practices, including tracking crop yield, environmental sustainability factors, pest risk analysis, livestock health and welfare monitoring, and even food safety and security.

Precision farming can be compromised by threats to data acquisition technologies and increased cyberattacks on farming systems (Threats to Precision Agriculture, 2018). Farming technologies and access to farm data attract the attention of cybercriminals who are looking to take advantage of vulnerabilities in the system for financial gain or other malicious intents (Amiri-Zarandi et al., 2020). Weaknesses in the system, fragmented technical security protocols, and human errors can allow attackers to easily access the farming network and the digital tools and introduce security breaches and risks. Security breach refers to unauthorized access and transmission of data which can result in leakage of sensitive, protected, or confidential information. Security breaches in the farming system may lead to compromising the entire system or bringing the network down allowing the attackers to control the entire system, and sabotage farm data or other assets. Coordinated attacks on a farming system can lead to stealing data, loss of proprietary information (such as contracts or security design), disruption to supply chain, or even reputation loss and financial loss.

West (2018) shares his view on security in farms and describes that there are two types of digital farming systems; those that have been hacked, and those that will be hacked in the future. Security of farms is hampered by the security attacks that are being prevalent and targeted in the agricultural sector. For example, the "REvil group" attacked and compromised the Dairy Farm Group's network, one of the largest retailers in Asia, and demanded roughly $30 million ransom and had access to the Dairy Farm network (Connor Madsen, 2021). Similarly, a hacking group, BlackMatter, carried out an attack on NEW Cooperative, a farmer cooperative, and locked up all the computer systems. BlackMatter demanded $5.9 million ransom and threatened to publish a terabyte of the cooperative's data. The company was forced to take their computer network offline to isolate the incursion. JBS, the world's largest meat-processing corporation based in Brazil, had to pay $11 million ransom since their computer network was hacked and the company was forced to temporarily shut down nine beef plants, disrupting meat processing across North America and Australia for an entire week. In 2019, HSBC issued a warning to farmers in the UK about the risks of cybercrime, such as phishing campaigns, ransomware attacks, and malware. Such security attacks can harm the agricultural sector and disrupt countries' economies that are highly reliant on agriculture.

Security attacks can result in security breaches which can have a detrimental effect. **Figure 1** provides a classification of security breaches. Security breaches can be caused intentionally or unintentionally on a farm system. For example, hacking is exploiting weaknesses in a network by a person who intentionally wants to penetrate the system (Gao and Zhong, 2015). Another example of an intentional attack is Malware. Malware is a software product designed to cause disruption in a network or system or gain unauthorized access to data (Rust et al., 2022). Ransomware is prevalent malware that attacks industries and new technologies that work with data. Ransomware can encrypt the files on a device and prevent users from accessing their information. The attackers usually display a ransom demand on the computer screen to release the locked information. Phishing is also a common cybersecurity scam that can harm farms' digital infrastructure (De Araujo Zanella et al., 2020; Van Der Linden et al., 2020). Through phishing, a hacker obtains some sensitive information through an email, phone call, or text message. Phishing can target an individual or a larger group of recipients and the attacker establishes a communication that seems to be a regular vendor of a business or a known contact. On the other hand, unintentional actions can also lead to many security breaches. Accidental data sharing, transmitting sensitive data without proper encryption, and unauthorized access to computing infrastructure resulting from wrong configurations are examples of unintentional threats. Unauthorized software installation and configuration errors are other examples of unintentional actions that may grant access to sensitive information or computing infrastructure (Cheng et al., 2017). Best practices and technology solutions that can protect farm systems from these threats are reviewed in the following sections.

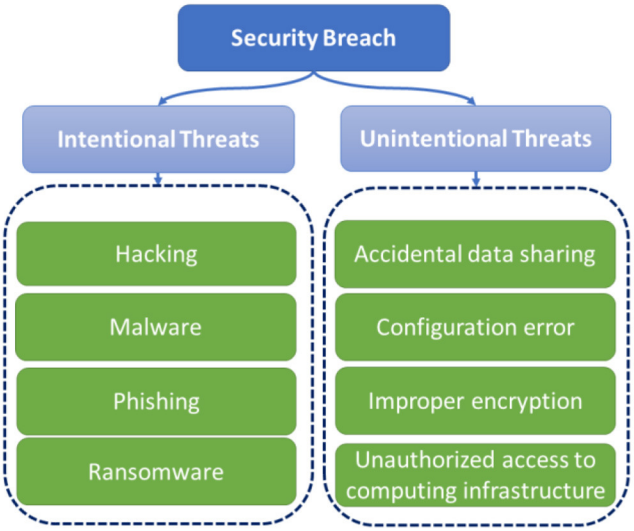

FIGURE 1 | Classification of security breaches.

Humans play a significant role in the security of IT infrastructure since attackers often use social engineering tactics to infiltrate or compromise a system. Hughes-Lartey et al. presented the relationship of security breach incidents and human factors (Hughes-Lartey et al., 2021). Human factors that can lead to security breaches include but are not limited to lack

of awareness, negligence, or using inappropriate access control practices. Moreover, studies show that employee negligence and insider involvement are the weakest links in an organization that may cause 95% of data breaches. These intentional or unintentional human errors can pose serious security risks.

As indicated above, farming systems are also vulnerable to cyber security attacks. Limited cybersecurity awareness among farmers, outdated security practices, lack of compliance with security standards, and prioritizing productivity on farms/farmers over the security of farm data are some of the reasons that can increase security attacks. Some research studies have also shown that there is a lack of emphasis on cybersecurity in the farming industry. Nikander et al. (2020) investigated the network and connected devices of six dairy farms in Finland and also conducted a survey of security practices at farms. The authors concluded that there is a significant need to improve farm system security at individual farm levels. They have also concluded that security threats are caused by farmers' activities or lack of activities, i.e., practicing security protection standards. Farm physical environment imposes its security challenges according to this study. Farmers in this survey have also expressed a lack of confidence in their ability to protect their farms against such attacks (Nikander et al., 2020). These findings suggest that enhancing farmers' awareness about security best practices can assist in safeguarding farm data and systems.

This paper provides a series of recommendations for farmers to improve security of farm IT infrastructure and farm data. We categorize our recommendations in three groups including human centered, technology-based and physical security for farmers. Furthermore, farm data cannot be effectively protected without reliable security technologies. In this paper, we elaborate on the important role ATPs or companies that build or govern farming systems and platforms can play to protect farm data. We also briefly review some of the security best practices and technologies that ATPs can provide or recommend to farmers. These recommendations can assist in enhancing system security and mitigating possible security risks and attacks.

SECURITY PRACTICES RECOMMENDED FOR FARMERS

Information security is an important requirement that farmers should pay careful attention to. Farmers should adopt security best practices to protect farm systems from potential cyber attacks. In general, the source of security issues can be divided into three categories: human error, technology, and physical aspects. Human errors refer to unintentional actions or lack of actions by users that allow a security breach to occur. Examples of such actions include downloading an email attachment containing malware, opening a phishing email, using weak passwords, and sharing personal passwords with others. As per IBM's report (IBM Security Services, 2014), human error is the root cause of 95% of security breaches. Technological security risks, such as ransomware and malware, are risks that are caused by software vulnerabilities, deficiencies in system design or setups, configuration errors, or other technology-related issues (e.g., lack of interoperability). Finally, physical data security issues are anything tangible that causes a security breach, such as unauthorized access to server rooms. Each of these security categories can cause irreparable damage to the farming system. **Figure 2** demonstrates these main causes of most security threats.

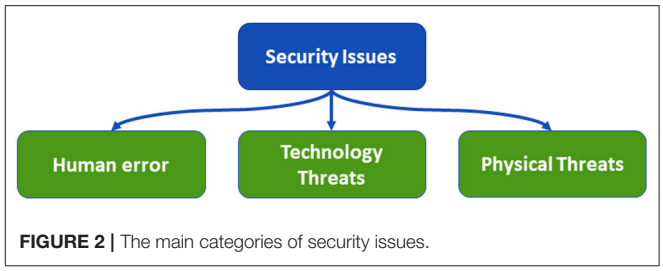

FIGURE 2 | The main categories of security issues.

In this section, we provide recommendations on security practices that can be adopted by farmers and farmworkers for each of the threat categories in **Figure 2**.

Human-Centered Solutions

Farmers as the end-users of farming technologies can be instrumental in securing farm IT infrastructure. Farmers and farmworkers' lack of awareness about potential security risks and practices may put farm technologies in a compromising security situation (Nikander et al., 2020). Several steps can be taken to tackle the human aspects of cybersecurity at farms which are imposed by the end-users. This section reviews these solutions.

Farmers should educate themselves and all farmworkers to improve their information security competency and to have a reasonably good level of awareness and vigilance. Furthermore, farmworkers should be trained to adopt day-to-day cybersecurity hygiene and best practices to take proactive steps in protecting farms' digital infrastructures such as servers, sensors, data, and other digital devices. For example, farmworkers should be trained and informed not to download apps from unknown or unreliable sources. They should also be aware of the harmful consequences of phishing emails. This can be achieved by showing examples of phishing emails and presenting the impacts of those emails. Farmworkers should be encouraged to report suspicious system performances to get help before other parts of the system are impacted (Hanus and Wu, 2016).

The common process to access a digital system is by using an authorized credential such as a username and password. Verizon states that the use of compromised or stolen credentials caused over 60% of security breaches in 2021 (Barr, 2021). This shows the importance of credential management practices such as password management and two-factor authentications. To prevent farm data from getting breached, farmers should work with ATPs to implement appropriate credential management and user authentication practices, e.g., passwordless or password-based practices. Through these practices, authorized users can be identified by their passwords or biometrics to prevent unauthorized access (Butler and Butler, 2014). Hackers can exploit weak, short, or exposed passwords to break into a system. If the system's authentication process is through passwords, using

TABLE 1 | Guidelines for creating strong passwords.

Guidelines to create and use strong passwords for authentication
1. Create a password longer than the recommended minimum required length by the system.
2. Use a combination of characters to create a password, including small and capital letters, numbers, and symbols.
3. Avoid choosing frequently-used words and personal information that are easy to guess (such as first/last name, pet name, or family member's name).
4. To remember the password, a random sentence and abbreviations can be used. Complexity can be added by capitalizing certain letters, such as "Take-Me2-Home!".
5. In case there is a need to write the passwords so that they are not forgotten, it is recommended to put the notes in a safe place.
6. Create separate usernames or passwords for different farm staff if possible.
7. Usernames or passwords should not be shared with others.
8. Change passwords periodically to alleviate the risk of compromise.
9. Do not save passwords or use auto-fill features on browsers.
10. If the system is compromised or it has been hacked, passwords should be changed immediately.
11. Change the default passwords of devices and machines at the farm while setting them up for the first time.
12. Use a random password generator or password management system if possible.

reliable passwords is one of the most effective precautions to keep access to the farm's digital infrastructure safe for authorized users. This can be achieved by defining strong passwords. **Table 1** contains recommendations for farmers and farmworkers to create strong passwords and to keep passwords secure.

Malware can impose different kinds of vulnerabilities on the digital systems installed at the farm. Malware is a program designed to gain unauthorized access to a network or system to steal information or cause damage to data or software. Malware can be distributed/downloaded by clicking on a link in an email, through a malicious website, or by executing a malicious file. Ransomware is one of the prevalent malware that can impact various sectors, including farming (West, 2018). One way of preventing malware such as ransomware, farmworkers should avoid opening suspicious emails, links, and files and should not connect to untrusted memory devices or computers. They should also avoid downloading software applications from unknown or untrusted sources on farm computing devices. Farmworkers should avoid signing in with their personal account on applications and websites online. They should also avoid linking online accounts to farm desktops, computers, or networks. Once an attacker gains access to an account associated with a device or network at the farm, they can use this channel to connect to other accounts or systems connected to a farm.

Phishing attacks are other prevalent threats in the farming ecosystem (Carneiro et al., 2021). Farmworkers should always be vigilant about potential social engineering traps such as phishing attacks, spam, and social media scams. Training farmworkers with practical examples by presenting past incidents and their consequences is a pragmatic way to raise awareness and prepare the staff to identify, avoid, or mitigate such attacks (Carneiro et al., 2021). It is also recommended not to click on links or open attachments embedded in suspicious emails. Farmworkers should further avoid sharing sensitive information with unknown/untrusted organizations or contacts. The source and purpose of information sharing should be clear and should be discussed with farm managers or ATPs.

Although some confidential data leakage incidents in a farm can be due to farmworkers' negligence or lack of action, in some cases, a data breach may take place intentionally by farm staff. Such incidents are referred to as insider attacks (Bae et al., 2011). In this type of attack, a disgruntled staff can sell confidential data to make a profit or disseminate data to cause harm. Proactive prevention of such attacks is crucial because the insider attackers have legitimate access to the system. Limiting those who have administrative access to the network, i.e., access privilege, and limiting the farmworkers' access to unrelated components of the farming system (Yang et al., 2020) that are not related to their work (e.g., data, devices, servers) can alleviate the risk of insider attacks. Access privilege can be set up by the ATPs through consultation with farm managers. For example, if a farm staff requires elevated, privileged access to the system, setting up a custom username-password and limiting permissions on what they can do can prevent unauthorized activities. Additionally, it is necessary to grant minimum access for farmworkers and only at a level that they can perform their job, which is also called zero trust (Campbell, 2020). If the work contract of a farm staff terminates and they are no longer associated with the farm operations, it is important to immediately revoke their access to farm computers, servers, and systems and change passwords even for emails (Data Security Policy, 2021). Also, if the farm staff has other work devices, such as a laptop or USB drive, those devices should be returned before quitting the job and remote access or other access privileges such as passwords should be deactivated to prevent unauthorized access to farm system.

In the case of an attack on the farm system and infrastructure, the passage of time can only worsen the situation. Therefore, it is highly recommended that farmers mitigate harm such as data leakage, system crashes, and compromised device or computer by seeking help from ATPs or farm insurances in the shortest amount of time possible. A response plan should be provided by ATPs for the farmers to execute the appropriate steps and detect and limit the damage and facilitate a quick recovery (Thompson, 2018). The plan should leverage all significant scenarios that could occur on farms. Also, it is suggested to prepare an on-call list of technology providers, technicians, and farmworkers who can respond to security events.

Technological Solutions

On-farm data acquisition technologies and other smart technologies can be susceptible to security risks. For this reason, appropriate technical measures should be taken to reduce vulnerabilities and secure the technological aspects of farms (Hamed et al., 2017). This section provides recommendations to farmers on the technology solutions they can obtain to secure data at farms.

A number of solutions can be implemented by the ATPs to protect farm computing infrastructure from such threats. For

instance, it is often the case that some farm operations are performed remotely. To do this, farmworkers need to connect to the farm network remotely to monitor, control, or perform a task with their own personal device. Setting up the heating system of the farm or turning off the irrigation system remotely while raining are examples of such remote activities. Personal devices are inherently insecure and may have unpatched vulnerabilities (Data Security Policy, 2021). In those cases, farmers can request access to farm computing infrastructure through Virtual Private Network (VPN). Farmworkers can use VPN to connect remotely to perform farm operations securely. Also, connecting from unsecured Wi-Fi networks such as open or public Wi-Fi can enable attackers to capture traffic off an open access point to perform attacks. Setting up multi-factor authentication can mitigate such security issues (Yang et al., 2020). Multi-factor authentication performs an additional sign-in method, such as sending a text or a number to your phone or email with a code to confirm the identity. Some authentication methods use a face ID (Fard and Hashemi, 2020) or fingerprint as an extra step after entering a username and password. The extra step to log in to the device or system can help protect the farming system from getting hacked or from unauthorized access. Protection from malware and ransomware can be improved by using antivirus software on all computers and laptops that are used at the farm. Furthermore, on-farm software devices need to be updated frequently. Automated updates can be set up to make the process easier.

IoT devices have different levels of security standards which are mentioned in device specifications (Matheu-García et al., 2019). Examples of digital farm devices include sensors, IoT irrigation systems, milking robots, and drones. Using devices with weak security levels, such as devices using unencrypted passwords, can increase the vulnerabilities of farm systems and networks. To mitigate this issue, it is recommended that farmers ask the technology providers about the farm devices' security features before they are installed at the farm. Farmers can also ask ATPs to enable the use of encryption for all data at rest or data in motion. It is recommended to list all equipment, hardware, and software available in the farm system and update the list when any new equipment is purchased. This list can help farmworkers to ensure all software and IoT devices firmware is up to date. Also, farmworkers can check the list periodically to find and uninstall unused software or devices (Matheu-García et al., 2019). Eliminating unused software and hardware and keeping available ones up to date can increase the security level of the entire agricultural system. Finally, if it is suspected that the system is infected with malware, it is recommended to disconnect the computer or device from the network to prevent the malware from spreading. The system should be scanned with an antivirus program. It is also recommended to ask ATPs to reinstall the system as the attacker can use some other techniques to access the compromised system.

Data loss in a farming system is a challenging issue that should be proactively addressed. Data loss can result from hardware or software problems, attacks on data, or accidental deletion of data. For example, malware and ransomware can lead to intentional data corruption and hardware or software problems (such as improper encryption) that can lead to unintentional data corruption (West, 2018). Backing up data regularly in the cloud and or other storage mediums off-farm is an easy approach to ensure that any issues with the data at farm do not impact the data backups (Thomas and Galligher, 2018). This strategy allows data to be restored from backup copies from an earlier point in time. Most of the recommendations provided in this section focus on adopting existing security standards and best practices by farmers to enhance security. To implement these or other technical solutions, farmers can ask the ATPs to install or activate these solutions or may recruit a trusted technician/consultant or seek technology providers' assistance to enhance data security in the farm system.

Physical Solutions

Issues arising from physical threats can also harm the farm system. This is a major threat for many farms given their open environment. The following are recommendations to secure physical space on the farm.

First of all, the farm entrance should be protected through digital locks or other means. It is also recommended that unauthorized entry should be strictly prohibited. Farmworkers should also be aware if they are expecting an outsider. For example, repair workers or maintenance workers should make prior arrangements for their visit to the farm. Farmworkers should not allow anyone to enter the premises without verifying their identity or purpose of visit. This can help in protecting farms from trespassing and access to main IT infrastructure, servers, routers, and other assets.

To monitor the physical barriers of the farm, surveillance equipment such as a security camera system, motion detector, and door alarms should be installed. It is also important to protect sensitive information, documents, and devices by placing them in secure spaces, such as locked cabinets, rooms, and off-site caches. Unnecessary copies of personal or sensitive data raise the risk of disclosure; therefore, they should be wiped or shredded. Moreover, physical access control and locking classified places can mitigate the risk of unauthorized access to devices and information.

Another physical security requirement is to protect electronic devices from failure. For example, since electronic devices and computers are vulnerable to dust, they need to be kept clean. This requires regular cleaning services of the electronic devices to decrease the risk of failure. Providing stable power as required for IoT devices and computers and installing regulators to reduce voltage fluctuation are other actions that can be taken to alleviate the risk of device failure.

THE ROLE OF AGRICULTURAL TECHNOLOGY PROVIDERS

Since ATPs design and deploy the technologies in farms, they can be instrumental in preventing potential security attacks and risks. Also, it is common that technology providers have access to digital infrastructure and information at the farm, such as farm networks, sensors, or data sources stored on-farm or in the

TABLE 2 | Practices that are recommended to ATPs.

Security practices recommended to Agricultural Technology Providers (ATPs)
1. Encrypt data transfer and data stored on devices and servers.
2. Keep operating systems and all software up to date to enable software patching.
3. Install and update virus scanners and malware detection software regularly.
4. Use firewalls on all computers and the entire network to protect against attacks. Ensure routers and firewalls are appropriately set up, configured and up to date.
5. Perform continuous vulnerability assessment, penetration test, and end-to-end monitoring in the entire farm system to monitor and address the shortcomings in advance (Threats to Precision Agriculture, 2018).
6. Install antivirus software to secure farm systems as well employee-owned devices (routers, phones, tablets, workstations, and servers) (Threats to Precision Agriculture, 2018).
7. Ensure controlled use of administrative privileges to prevent unauthorized access to sensitive data.
8. Utilize user authentication mechanisms, e.g., multi-factor authentication (Ometov et al., 2018), to validate user identity when accessing common cloud services.
9. Enable "privileged access" control to farm data to protect sensitive information and ease access to less sensitive information that are used frequently for farm management.
10. Ensure the Wi-Fi connection is private and regularly monitor it to prevent attackers from accessing sensitive data. Remote access through VPN can also be enabled.
11. Use secure channel and communication protocols for all connections and data transfers.
12. Use automatic session timeout and configuration to automatically log out after a defined time to decrease the risk of illegal access to farm system (Carneiro et al., 2021).
13. Provide data recovery capabilities as well as a reliable backup system.
14. Use de-identification at source techniques from the first steps of data collection to protect farmers' privacy (Zaman et al., 2016).
15. Prepare incident response and disaster recovery plans to manage potential risks in the system.
16. Use emerging technologies such as blockchain or passwordless authentication systems.

cloud. This means that working with a trusted ATP is critical in providing the required security level in the farm system.

Adopting information security standards by ATPs in precision farming systems is important for implementing a highly secure environment (Threats to Precision Agriculture, 2018). Security standards and practices should be embedded as a default feature in the digital IT architecture and design (Vallois et al., 2019). Security by design recommends a set of standards that can be used in all the application development (or installation) stages, from requirement analysis, implementation, and all the way to production. User-friendliness of these features is important to encourage use and adoption by farmers and farmworkers as they will be more intuitive to learn and remember. For example, using a secure, easy to use, and effective biometric or password management system for logging in instead of using traditional passwords can simplify access to systems in a secure manner and reduce the possibility of unauthorized access or errors (Obaidat et al., 2019). Also, designing a logout button in applications to remind farm staff to log out of the system while leaving or an automatic log out function can assist with locking the system when they are not in use by authorized staff.

The software on the farm devices should be kept up to date to protect from malware and ransomware. Since having up-to-date software decreases the risk of security threats, it would be best to set the computers, tablets, cell phones, and other digital devices to update software automatically. ATPs should provide farmers with instructions on how to install and update security software tools. It is also essential to install reliable firewalls on the systems and entire network to keep them up to date all the time (Cain et al., 2018). A firewall is a network security software or device that can monitor incoming and outgoing traffic to the network and filter suspicious activities based on security rules and machine learning based detectors.

ATPs can use security enhancing tools on the farm system or network to detect insider attacks and inform farmers about possible threats proactively. Enabling software tools that can monitor network activity from time to time and checking for suspicious activities are important to secure the farm system and network. For example, access to a farm system after work hours can be an indication of illegitimate behavior. Also, ATPs can use a location-based key management method to combat insider threats (Choi et al., 2015). This method automatically monitors the location of the person who tries to access the system remotely. In the case of suspicious or unknown locations, it asks for stronger authorization methods to ensure legitimate access to the system (Alneyadi et al., 2016).

After designing the farm system, ATPs can mitigate security risks in the farm by performing vulnerability assessments and penetration testing. Vulnerability assessment can identify vulnerabilities in the system and create a set of recommendations to fix them (Alhazmi and Malaiya, 2005). This identification can help prevent risks to the entire network and infrastructures of a digital farming environment that may impact farm operations and processes. Furthermore, penetration testing simulates an attack to assess the security level of a system (Bacudio et al., 2011). This complementary testing mechanism helps farm staff and the entire system to be prepared for potential cybersecurity issues in advance. In addition, using proper encryption for all data transfers and data stored at farm servers is a secure mechanism to protect from security breaches and risks.

With the rise of emerging technologies such as blockchain and passwordless authentication systems, ATPs can consider these technology solutions to protect farm data. Blockchain is a distributed database and immutable ledger that enables secure transactions and transfer of ownership. It also ensures transparency and trust among stakeholders (Xiong et al., 2020). Blockchain can ensure privacy of transactions, ownership rights, and provide greater control of data for farmers by enabling an effective mechanism for identity management. Passwordless authentication mechanism is an effective way to validate identity of the user and allow secure access to computing infrastructure at the farm. They have shown to be more user-friendly than passwords and can improve compatibility (e.g., interoperability) (Parmar et al., 2022).

Table 2 provides recommendations on security practices that ATPs can adopt to secure farm data and digital infrastructure.

CONCLUSION

Security breaches can cause irreparable harm to farmers. The consequences of security threats include, but are not limited to, stealing information, reputation loss, destruction of equipment, error in system configuration and performance, and gaining an improper financial advantage over a competitor. Existing research suggests that 95% of security breaches are caused by humans. In addition, past research by Hanus and Wu (2016) has shown that farmers are not aware of security practices that can be used to protect their farms.

This gap suggests the need for security standards that can be applied to protect farms. Connectivity of farm systems with other systems such as smart cities, supply chain, and other smart facilities enforces the necessity for securing digital infrastructures at farms. In addition, many countries have considered agriculture as the critical national infrastructure that requires extra protection. The objective of this paper is to provide recommendations on the adoption of existing security best practices by farmers and ATPs to prevent security breaches and sensitive data leakage. For the farmers, recommendations were provided in three categories of human errors, physical threats, and technology threats. ATPs can secure the farm digital infrastructure by adopting standards for securing technology, process, and protocols. The role of governments is also important to enforce policies and principles related to farm data security. As for the future direction, we will work with the national farm associations to present this research in a usable format for farmers. We expect that farmers' trust and long-lasting relationship with these associations will enhance an adoption of the recommended security practices (Rust et al., 2022).

AUTHOR CONTRIBUTIONS

MH and RD contributed to conception of the study. All authors have contributed to writing the paper, manuscript revision, read, and approved the submitted version.

FUNDING

This research was funded by a Natural Sciences and Engineering Research Council of Canada (NSERC) Discovery Grant and Ontario Ministry of Agriculture Food and Rural Affairs, New Directions, funding awarded to RD.

REFERENCES

Alhazmi, O. H., and Malaiya, Y. K. (2005). "Quantitative vulnerability assessment of systems software," in *Annual Reliability and Maintainability Symposium, 2005. Proceedings*, 615–620.

Alneyadi, S., Sithirasenan, E., and Muthukkumarasamy, V. (2016). A survey on data leakage prevention systems. *J. Netw. Comput. Appl.* 62, 137–152. doi: 10.1016/j.jnca.2016.01.008

Amiri-Zarandi, M., Dara, R. A., and Fraser, E. (2020). A survey of machine learning-based solutions to protect privacy in the Internet of Things. *Comput. Sec.* 96, 101921. doi: 10.1016/j.cose.2020.101921

Bacudio, A. G., Yuan, X., Chu, B.-T. B., and Jones, M. (2011). An overview of penetration testing. *Int. J. Netw. Sec. Appl.* 3, 19. doi: 10.5121/ijnsa.2011.3602

Bae, K., Kim, S., Lee, Y., You, I., Yim, K., and Son, T. (2011). "Insider threats are getting worse within industries: isolated secondary backup required," in *2011 Third International Conference on Intelligent Networking and Collaborative Systems* 652–655. doi: 10.1109/INCoS.2011.165

Barr, B. (2021). *Data Breach Investigations Report. Credential Stuffing, Data Breaches, Malware*. Avaialbe online at: https://spycloud.com/highlights-from-the-verizon-2021-data-breach-investigations-report/#:$\sim$:text=Criminals Want Credentials,cause of all data breaches.andtext=According to Verizon%2C 61%25 of,25%25 of breaches last year (accessed January 28, 2021).

Butler, R., and Butler, M. (2014). "An assessment of the human factors affecting the password performance of South African online consumers," in *HAISA*, 150–161.

Cain, A. A., Edwards, M. E., and Still, J. D. (2018). An exploratory study of cyber hygiene behaviors and knowledge. *J. Inf. Sec. Appl.* 42, 36–45. doi: 10.1016/j.jisa.2018.08.002

Campbell, M. (2020). Beyond zero trust: trust is a vulnerability. *Computer* 53, 110–113. doi: 10.1109/MC.2020.3011081

Carneiro, R., Duncan, S., Ramsey, F., Seyyedhasani, H., and Murch, R. (2021). *Cyber Attacks in Agriculture: Protecting Your Farm and Small Business With Cyberbiosecurity*. Virgina: VCE Publications.

Cheng, L., Liu, F., and Yao, D. (2017). Enterprise data breach: causes, challenges, prevention, and future directions. *Wiley Interdiscip. Rev.: Data Min. Knowl. Discov.* 7, e1211. doi: 10.1002/widm.1211

Choi, J., Bang, J., Kim, L., Ahn, M., and Kwon, T. (2015). Location-based key management strong against insider threats in wireless sensor networks. *IEEE Syst. J.* 11, 494–502. doi: 10.1109/JSYST.2015.2422736

Cisternas, I., Velásquez, I., Caro, A., and Rodriguez, A. (2020). Systematic literature review of implementations of precision agriculture. *Comput. Electron. Agric.* 176, 105626. doi: 10.1016/j.compag.2020.105626

Connor Madsen (2021). *Cyber News Rundown: Dairy Farm Ransomware*. Available online at: https://www.webroot.com/blog/2021/02/03/cyber-news-rundown-dairy-farm-ransomware/ (accessed December 10, 2021).

Data Security Policy (2021). *Risk Management Practice Guide of Lawyers Mutual*. Avaialbe online at: https://nmcdn.io/e186d21f8c7946a19faed23c3da2f0da/556712d9bf0f4cb2a916cc810687d52b/files/risk-management-resources/practice-guides/Data_Security_Policy.pdf (accessed December 15, 2021).

De Araujo Zanella, A. R., da Silva, E., and Albini, L. C. P. (2020). Security challenges to smart agriculture: current state, key issues, and future directions. *Array* 8, 100048. doi: 10.1016/j.array.2020.100048

Fard, S. M. H., and Hashemi, S. (2020). Proposing a sparse representational based face verification system to run in a shortage of memory. *Multimed. Tools Appl.* 79, 2965–2985. doi: 10.1007/s11042-019-08491-3

Gao, X., and Zhong, W. (2015). Information security investment for competitive firms with hacker behavior and security requirements. *Ann. Oper. Res.* 235, 277–300. doi: 10.1007/s10479-015-1925-2

Hamed, T., Dara, R., and Kremer, S. C. (2017). "Intrusion detection in contemporary environments," in *Computer and Information Security Handbook*, ed J. R. Vacca (Burlington, MA: Elsevier), 109–130. doi: 10.1016/B978-0-12-803843-7.00006-5

Hanus, B., and Wu, Y. (2016). Impact of users' security awareness on desktop security behavior: A protection motivation theory perspective. *Inf. Syst. Manag.* 33, 2–16. doi: 10.1080/10580530.2015.1117842

Hughes-Lartey, K., Li, M., Botchey, F. E., and Qin, Z. (2021). Human factor, a critical weak point in the information security of an organization's Internet of things. *Heliyon* 7, e06522. doi: 10.1016/j.heliyon.2021.e06522

IBM (2021). *IBM AI and Cloud Technology Helps Agriculture Industry Improve the World's Food and Crop Supply*. IBM. Avaialbe online at: https://newsroom.ibm.com/2019-05-22-IBM-AI-and-Cloud-Technology-Helps-Agriculture-

Industry-Improve-the-Worlds-Food-and-Crop-Supply (accessed January 8, 2021).

IBM Security Services 2014 Cyber Security Intelligence Index. (2014). *Analysis of Cyber Attack and Incident Data from IBM's Worldwide Security Operations*. Armonk, NY: IBM Global Technology Services. Available online at: https://i.crn.com/sites/default/files/ckfinderimages/userfiles/images/crn/custom/IBMSecurityServices2014.PDF

MarketsandMarkets (2022). Avaialbe online at: https://www.marketsandmarkets.com/Market-Reports/precision-farming-market-1243.html (accessed May 20, 2022).

Matheu-García, S. N., Hernández-Ramos, J. L., Skarmeta, A. F., and Baldini, G. (2019). Risk-based automated assessment and testing for the cybersecurity certification and labelling of IoT devices. *Comput. Stand. Interfaces* 62, 64–83. doi: 10.1016/j.csi.2018.08.003

Nikander, J., Manninen, O., and Laajalahti, M. (2020). Requirements for cybersecurity in agricultural communication networks. *Comput. Electron. Agric.* 179, 105776. doi: 10.1016/j.compag.2020.105776

Obaidat, M. S., Rana, S. P., Maitra, T., Giri, D., and Dutta, S. (2019). "Biometric security and internet of things (IoT)," in *Biometric-Based Physical and Cybersecurity Systems*, ed M. S. Obaidat, I. Traore, I. Woungang (Cham: Springer), 477–509. doi: 10.1007/978-3-319-98734-7_19

Ometov, A., Bezzateev, S., Mäkitalo, N., Andreev, S., Mikkonen, T., and Koucheryavy, Y. (2018). Multi-factor authentication: a survey. *Cryptography* 2, 1. doi: 10.3390/cryptography2010001

Parmar, V., Sanghvi, H. A., Patel, R. H., and Pandya, A. S. (2022). "A comprehensive study on passwordless authentication," in *International Conference on Sustainable Computing and Data Communication Systems (ICSCDS)*. doi: 10.1109/ICSCDS53736.2022.9760934

Rust, N., Stankovics, P., Jarvis, R. M., Morris-Trainor, Z., de Vries, J. R., Ingram, J., et al. (2022). Have farmers had enough of experts? *Environ. Manag.* 69, 31–44. doi: 10.1007/s00267-021-01546-y

Thomas, J., and Galligher, G. (2018). Improving backup system evaluations in information security risk assessments to combat ransomware. *Comput. Inf. Sci.* 11. doi: 10.5539/cis.v11n1p14

Thompson, E. C. (2018). *Cybersecurity Incident Response: How to Contain, Eradicate, and Recover From Incidents*. Apress. doi: 10.1007/978-1-4842-3870-7

Threats to Precision Agriculture (2018). Avaialbe online at: https://www.dhs.gov/sites/default/files/publications/2018AEP_Threats_to_Precision_Agriculture.pdf (accessed November 30, 2021).

Vallois, V., Guenane, F., and Mehaoua, A. (2019). "Reference architectures for security-by-design iot: Comparative study," in *2019 Fifth Conference on Mobile and Secure Services (MobiSecServ)*, 1–6. doi: 10.1109/MOBISECSERV.2019.8686650

Van Der Linden, D., Michalec, O. A., and Zamansky, A. (2020). Cybersecurity for smart farming: socio-cultural context matters. *IEEE Technol. Soc. Mag.* 39, 28–35. doi: 10.1109/MTS.2020.3031844

West, J. (2018). A prediction model framework for cyber-attacks to precision agriculture technologies. *J. Agric. Food Inf.* 19, 307–330. doi: 10.1080/10496505.2017.1417859

Xiong, H., Dalhaus, T., Wang, P., and Huang, J. (2020). Blockchain technology for agriculture: applications and rationale. *Front. Blockchain* 3:7. doi: 10.3389/fbloc.2020.00007

Yang, X., Shu, L., Chen, J., Ferrag, M. A., Wu, J., Nurellari, E., et al. (2020). A survey on smart agriculture: development modes, technologies, and security and privacy challenges. *IEEE/CAA J. Automat. Sin.* 8, 273–302. doi: 10.1109/JAS.2020.1003536

Zaman, A. N. K., Obimbo, C., and Dara, R. A. (2016). "A novel differential privacy approach that enhances classification accuracy," in *Proceedings of the Ninth International C* Conference on Computer Science and Software Engineering*, 79–84. doi: 10.1145/2948992.2949027

Conflict of Interest: The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's Note: All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.