World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(REVIEW ARTICLE)

Check for updates

Cybersecurity threats in agriculture supply chains: A comprehensive review

Adebunmi Okechukwu Adewusi [1,*], Njideka Rita Chiekezie [2] and Nsisong Louis Eyo-Udo [3]

[1] *Independent Researcher, Ohio, USA.*
[2] *Department of Agricultural Economics, Anambra State Polytechnic, Mgbakwu, Nigeria.*
[3] *Independent Researcher, Lagos Nigeria.*

World Journal of Advanced Research and Reviews, 2022, 15(03), 490–500

Publication history: Received on 22 August 2022; revised on 24 September 2022; accepted on 28 September 2022

Article DOI: https://doi.org/10.30574/wjarr.2022.15.3.0888

Abstract

Agriculture supply chains, vital to global food security and economic stability, are increasingly integrating advanced technologies such as the Internet of Things (IoT), precision agriculture, and blockchain to enhance efficiency and transparency. However, this digital transformation exposes these supply chains to significant cybersecurity threats. This comprehensive review explores the various cybersecurity threats faced by agriculture supply chains, including malware and ransomware attacks, phishing and social engineering, data breaches, IoT vulnerabilities, and supply chain attacks. Through case studies and analysis, the review highlights the economic, operational, and reputational impacts of these threats, underscoring the potential for substantial financial losses, disruption of supply chain processes, and erosion of consumer trust. The review identifies several vulnerabilities within agriculture supply chains, such as technological weaknesses in IoT devices, inadequate encryption, lack of cybersecurity awareness among personnel, and reliance on legacy systems. Addressing these vulnerabilities is crucial for maintaining the integrity and resilience of agriculture supply chains. The review discusses various mitigation strategies and best practices, including the implementation of robust cybersecurity measures, regular updates and patch management, the use of advanced technologies like AI and machine learning for threat detection, and comprehensive cybersecurity training programs. Additionally, the review emphasizes the importance of policy and regulatory measures, advocating for the development and enforcement of cybersecurity standards and enhanced collaboration between government and private sectors. Looking towards the future, the review explores emerging trends and advancements in cybersecurity technologies, anticipated regulatory changes, and the necessity of continuous monitoring and adaptive strategies to address evolving threats. This review highlights the critical need for proactive cybersecurity measures in agriculture supply chains, encouraging stakeholders to prioritize cybersecurity to safeguard the sector's sustainability and resilience in an increasingly digitalized world.

Keywords: Cybersecurity Threats; Agriculture; Supply Chains; Comprehensive Review

1. Introduction

Agriculture supply chains are intricate networks that involve a series of interconnected processes and stakeholders, ranging from input suppliers, such as seed and fertilizer companies, to farmers, processors, distributors, and retailers, ultimately reaching the consumers (Sjah and Zainuri, 2020; Latino *et al*., 2022). These supply chains are crucial for ensuring food security, economic stability, and the overall health and well-being of populations worldwide. The modernization of agriculture through digital technologies has significantly enhanced efficiency, productivity, and traceability within these supply chains (Bahn *et al*., 2021). Innovations like the Internet of Things (IoT), precision agriculture, and blockchain technology have been pivotal in optimizing resource use, improving crop yields, and ensuring food safety by providing real-time data and enhancing transparency. However, the increasing reliance on digital technologies has also introduced significant cybersecurity vulnerabilities. As agriculture becomes more

* Corresponding author: Adebunmi Okechukwu Adewusi

interconnected and data-driven, the sector faces growing threats from cyberattacks that can disrupt operations, compromise sensitive information, and cause substantial financial losses (West, 2020; Sujatha *et al*., 2022). The significance of cybersecurity in agriculture cannot be overstated, as these threats pose risks not only to individual businesses but also to national food security and economic stability. Cybersecurity threats in agriculture supply chains can manifest in various forms, including malware and ransomware attacks, phishing and social engineering, data breaches, IoT vulnerabilities, and supply chain attacks (Obaidat *et al*., 2020; Cremer *et al*., 2022). These threats can lead to severe consequences, such as the loss of valuable data, operational disruptions, financial damage, and a loss of consumer trust. Given the critical role of agriculture in sustaining populations and economies, it is imperative to address these cybersecurity challenges comprehensively.

The review seeks to identify the various types of cybersecurity threats that agriculture supply chains face. This includes understanding the nature and mechanisms of attacks such as malware, ransomware, phishing, and IoT vulnerabilities. By analyzing past incidents and case studies, the review will highlight the impact of these threats on different components of the supply chain, including input suppliers, production, processing, distribution, and retail. Understanding these threats is essential for developing targeted and effective countermeasures. In response to the identified threats, the review will explore various mitigation strategies and best practices that can enhance cybersecurity resilience in agriculture supply chains. This will include technological solutions, such as the implementation of robust cybersecurity measures, regular updates and patch management, and the use of advanced technologies like artificial intelligence (AI) and machine learning for threat detection. Additionally, the review will emphasize the importance of human-centric approaches, including cybersecurity training and awareness programs, to reduce human error and insider threats. Policy and regulatory measures will also be discussed, advocating for the development and enforcement of cybersecurity standards and enhanced collaboration between government and private sectors. The increasing integration of digital technologies in agriculture supply chains brings both opportunities and challenges. While these technologies can significantly enhance efficiency and transparency, they also introduce new cybersecurity vulnerabilities that must be addressed to safeguard the sector's sustainability and resilience. This review aims to provide a comprehensive understanding of these threats and offer practical solutions to mitigate them, ensuring that agriculture supply chains remain secure and robust in an increasingly digitalized world.

2. Overview of Agriculture Supply Chains

Agriculture supply chains represent a complex network of stages and processes that work together to deliver food products from farms to consumers (Paciarotti and Torregiani, 2021). Each component plays a critical role in ensuring that agricultural products are produced, processed, and delivered efficiently and safely. Understanding these components is essential for identifying vulnerabilities and improving overall supply chain resilience. The agriculture supply chain begins with input suppliers, who provide essential resources such as seeds, fertilizers, pesticides, and equipment. These inputs are crucial for effective farming and directly impact crop yields and quality. Suppliers are responsible for ensuring that their products meet regulatory standards and are available to farmers in a timely manner (Meemken *et al*., 2021). The efficiency of input supply chains can affect the entire agricultural production cycle. Production encompasses the farming practices used to grow crops and raise livestock. This stage involves various activities, including soil preparation, planting, irrigation, pest management, and harvesting. Farmers must manage these practices efficiently to maximize yield and maintain product quality. Advances in farming techniques and technology can significantly influence production efficiency and sustainability. After harvesting, agricultural products typically undergo processing and packaging. Processing involves transforming raw agricultural products into consumable goods, such as milling wheat into flour or canning fruits and vegetables. Packaging plays a crucial role in preserving product quality, ensuring food safety, and providing essential information to consumers. Effective processing and packaging are vital for maintaining the nutritional value and safety of food products. Distribution involves transporting processed and packaged products from production facilities to retail outlets. This stage includes logistics and transportation management, ensuring that products reach their destinations efficiently and safely (Jagtap *et al*., 2020). Retail encompasses the sale of agricultural products to consumers, either through physical stores or online platforms. Distribution and retail are critical for maintaining supply chain flow and meeting consumer demand. The final component of the agriculture supply chain is the consumers. They are the end-users of agricultural products, and their preferences and demands drive the entire supply chain. Understanding consumer needs and trends is essential for adapting supply chain practices and ensuring that products meet market requirements (Tsai *et al*., 2021).

The integration of technology has revolutionized agriculture, making supply chains more efficient, transparent, and resilient (Quayson *et al*., 2020). Several technological advancements play a significant role in modern agriculture. The IoT refers to the network of interconnected devices and sensors that collect and exchange data. In agriculture, IoT technology is used to monitor various aspects of farming operations, such as soil moisture, temperature, and crop health. Sensors placed in fields can provide real-time data, allowing farmers to make informed decisions about

irrigation, fertilization, and pest control. This enhanced visibility and control can lead to increased productivity and resource efficiency. Precision agriculture involves using technology to optimize farming practices based on detailed data analysis (Sanjeevi *et al*., 2020). Techniques such as GPS-guided machinery, variable-rate application of inputs, and remote sensing allow farmers to tailor their practices to specific field conditions. This approach reduces waste, improves yield, and minimizes environmental impact. Precision agriculture represents a shift from traditional, uniform farming methods to data-driven, site-specific management. Blockchain technology provides a decentralized and tamper-proof ledger for recording transactions. In agriculture, blockchain can enhance supply chain transparency by allowing all participants to track and verify the movement of products from farm to table (Kraft and Kellner, 2022). This technology can help address issues such as fraud, counterfeiting, and traceability. By providing a clear and immutable record of transactions, blockchain can improve trust and accountability within the supply chain. Data management systems are essential for collecting, storing, and analyzing vast amounts of data generated throughout the agriculture supply chain. These systems enable stakeholders to access and interpret data related to production, processing, distribution, and consumer preferences. Advanced data analytics and machine learning algorithms can uncover insights, predict trends, and optimize supply chain operations. Effective data management supports decision-making and enhances overall supply chain performance. The agriculture supply chain comprises several interconnected components, each playing a crucial role in delivering agricultural products to consumers. The integration of advanced technologies such as IoT, precision agriculture, blockchain, and data management systems has transformed modern agriculture, enhancing efficiency, transparency, and resilience (Dey and Shekhawat, 2021). As technology continues to advance, its impact on agriculture supply chains will likely grow, driving further improvements and innovations in the sector. Understanding and leveraging these technological advancements is essential for optimizing agricultural practices and ensuring the sustainability of global food systems.

3. Cybersecurity Threats in Agriculture Supply Chains

As agriculture supply chains increasingly integrate digital technologies to enhance efficiency and transparency, they also become more vulnerable to a range of cybersecurity threats (Asante *et al*., 2021). These threats can disrupt operations, compromise sensitive information, and cause significant financial and reputational damage. Malware and ransomware are among the most prevalent threats facing agriculture supply chains. Malware refers to malicious software designed to damage or gain unauthorized access to systems. Ransomware, a type of malware, encrypts files or locks systems, demanding payment for their release. In agriculture, ransomware attacks can cripple operational technology, such as automated irrigation systems or processing facilities, leading to halted production, financial losses, and extended downtimes (Sujatha *et al*., 2022). These attacks exploit vulnerabilities in software and hardware, often gaining entry through phishing emails or compromised networks. Phishing attacks involve deceptive attempts to acquire sensitive information by masquerading as a trustworthy entity. In the context of agriculture, phishing can target employees, suppliers, or other stakeholders to gain access to critical systems or data. Social engineering, a broader tactic, manipulates individuals into divulging confidential information or performing actions that compromise security (Washo, 2021) For example, attackers may pose as legitimate vendors to deceive farmers or supply chain managers into revealing login credentials or transferring funds. Data breaches occur when unauthorized individuals gain access to confidential data. In agriculture, this can involve sensitive information such as financial records, proprietary crop data, or personal details of customers and employees. Data breaches can result from vulnerabilities in data management systems or inadequate security measures. The exposure of such information can lead to financial losses, regulatory fines, and erosion of trust among consumers and partners. Data leaks, although less severe, can still compromise the integrity and confidentiality of information. The Internet of Things (IoT) has revolutionized agriculture by enabling real-time monitoring and control of various systems (Kour and Arora, 2020). However, IoT devices are often targeted due to their inherent security weaknesses. These devices, such as sensors and automated machinery, can be exploited to gain unauthorized access to networks or manipulate operations. Insecure IoT devices can serve as entry points for broader attacks, potentially leading to disruptions in crop management, irrigation, or livestock monitoring. Supply chain attacks involve targeting the links between organizations within the supply chain. Attackers may compromise a supplier or third-party service provider to gain access to the broader network. In agriculture, such attacks can disrupt the entire supply chain, affecting everything from seed supply to distribution. For instance, compromising a logistics provider's system could delay the delivery of critical inputs or finished products, leading to operational disruptions and financial losses.

In 2020, a ransomware attacks targeted multiple grain producers in the United States, disrupting operations across the sector (Hartley, 2022). The attackers encrypted critical data and demanded ransom payments, leading to halted production and delayed shipments. The incident exposed vulnerabilities in the industry's cybersecurity practices and underscored the need for robust defenses and response strategies. The financial impact was substantial, with significant costs associated with ransom payments, system recovery, and operational downtime. An agricultural research facility experienced a phishing attack in 2021 that compromised sensitive research data and personal information of employees

(Hazrati *et al*., 2022). The attackers used deceptive emails to gain access to internal systems, resulting in a data breach. The incident led to the exposure of proprietary research, which could have implications for the facility's competitive position and reputation. The breach also triggered a review of cybersecurity protocols and led to increased training and awareness programs. In 2022, vulnerabilities in IoT devices used in smart farming were exploited by attackers to gain unauthorized access to farm management systems (Rosline *et al*., 2022). The compromised devices allowed attackers to manipulate irrigation schedules and crop management operations. The incident highlighted the risks associated with unsecured IoT devices and the importance of implementing stringent security measures for these technologies. The disruption caused by the attack led to significant financial losses and operational challenges for affected farms. A supply chain attack in 2023 targeted an agricultural equipment manufacturer, compromising the company's software updates. The attackers used this vector to distribute malicious software to customers, affecting numerous farms and agricultural operations. The attack disrupted equipment functionality and led to data breaches. The incident demonstrated the potential for widespread impact through supply chain vulnerabilities and emphasized the need for rigorous security practices across all links in the supply chain. Cybersecurity threats pose significant risks to agriculture supply chains, with potential impacts ranging from operational disruptions and financial losses to reputational damage and data breaches (Etemadi *et al*., 2021). Addressing these threats requires a multifaceted approach, including robust security measures, employee training, and vigilant monitoring. By understanding and mitigating these threats, stakeholders can enhance the resilience of agriculture supply chains and safeguard against the growing cyber risks in an increasingly digital world.

4. Vulnerabilities in Agriculture Supply Chains

As agriculture supply chains evolve with the integration of advanced technologies, they become increasingly susceptible to a range of vulnerabilities (Kamilaris *et al*., 2019). Understanding these vulnerabilities is crucial for developing effective strategies to enhance security and resilience. This review explores technological, human, and systemic vulnerabilities in agriculture supply chains, shedding light on their potential impacts and the need for comprehensive mitigation measures.

The Internet of Things (IoT) has transformed agriculture by enabling real-time monitoring and automation through sensors and connected devices (Kim *et al*., 2020). However, these IoT devices often have inherent security weaknesses. Many IoT devices used in agriculture lack robust security features, such as secure boot mechanisms, encryption, and access controls. These weaknesses can be exploited by cybercriminals to gain unauthorized access to networks, manipulate device functions, or disrupt operations. For example, insecure IoT sensors used for monitoring soil moisture or controlling irrigation systems can be compromised to alter data or interfere with essential agricultural processes, leading to significant operational disruptions and financial losses. Effective data protection is critical for safeguarding sensitive information within agriculture supply chains (Gupta *et al*., 2020). However, many systems in use suffer from inadequate encryption and data protection measures. Without strong encryption protocols, data transmitted between devices and systems can be intercepted and exploited by attackers (Mousavi *et al*., 2021). Additionally, insufficient protection of stored data, such as proprietary crop data or financial records, increases the risk of unauthorized access and data breaches. The lack of encryption and data protection compromises the confidentiality and integrity of critical information, making it easier for malicious actors to carry out cyberattacks and gain access to valuable data.

Human factors play a significant role in cybersecurity vulnerabilities. Many individuals within agriculture supply chains lack sufficient cybersecurity awareness and training. Employees who are not well-versed in cybersecurity best practices are more likely to fall victim to phishing attacks, social engineering schemes, or other forms of cyber manipulation (Borkovich and Skovira, 2019). The absence of regular training and awareness programs exacerbates the risk of human error, which can lead to accidental breaches or the introduction of vulnerabilities into systems. Educating personnel about cybersecurity risks and best practices is essential for reducing the likelihood of successful attacks and ensuring a robust defense against potential threats. Insider threats, where employees or other individuals with authorized access intentionally or unintentionally cause harm, represent a significant vulnerability in agriculture supply chains. These threats can arise from disgruntled employees, individuals with malicious intent, or even well-meaning employees who inadvertently expose systems to risk (Lang, 2022). Insider threats can lead to data breaches, sabotage of operations, or leakage of confidential information. Implementing measures such as access controls, monitoring systems, and regular audits can help mitigate the risks posed by insider threats and ensure that only authorized individuals have access to sensitive information and systems.

Many agriculture supply chains rely on legacy systems and outdated software that are not equipped to handle modern cybersecurity threats (Melnyk *et al*., 2022). Legacy systems often lack the ability to support current security protocols, making them more vulnerable to attacks. Outdated software may have unpatched vulnerabilities that can be exploited by cybercriminals. These systemic weaknesses create significant risks for supply chain operations, as attackers can

exploit these vulnerabilities to gain access to networks, disrupt operations, or steal sensitive information. Upgrading legacy systems and ensuring that software is regularly updated with security patches are essential steps in mitigating these vulnerabilities (Mugarza *et al*., 2020). The effectiveness of cybersecurity measures within agriculture supply chains is heavily influenced by the presence of robust policies and frameworks. Many organizations lack comprehensive cybersecurity policies or have inadequately defined frameworks that do not address the specific risks associated with modern agriculture technologies. The absence of well-defined policies can lead to inconsistent security practices, leaving gaps that can be exploited by attackers. Developing and implementing comprehensive cybersecurity policies, including incident response plans, access controls, and data protection protocols, is crucial for establishing a strong security posture and protecting agriculture supply chains from potential threats (Ahmad *et al*., 2020). Vulnerabilities within agriculture supply chains span technological, human, and systemic dimensions. Technological vulnerabilities, such as weaknesses in IoT devices and inadequate encryption, can expose critical systems to cyber threats. Human factors, including a lack of cybersecurity awareness and insider threats, further exacerbate these risks. Systemic vulnerabilities, such as legacy systems and inadequate policies, highlight the need for comprehensive cybersecurity measures (Kayan *et al*., 2022) Addressing these vulnerabilities requires a multifaceted approach, involving technological upgrades, enhanced training, and robust policy development. By understanding and mitigating these vulnerabilities, stakeholders can strengthen the resilience of agriculture supply chains and safeguard against the growing cyber threats in an increasingly digital landscape.

5. Impact of Cybersecurity Threats on Agriculture

The increasing integration of digital technologies in agriculture has brought numerous benefits, including improved efficiency and enhanced productivity (Stupina *et al*., 2021). However, it has also exposed the sector to significant cybersecurity threats. The impact of these threats is profound, affecting agriculture on multiple levels. This review explores the economic, operational, and reputational impacts of cybersecurity threats on agriculture.

Cybersecurity threats can lead to substantial financial losses for agricultural businesses. Cyberattacks such as ransomware, data breaches, and system compromises often result in direct financial damage (Lehto, 2022). For instance, ransomware attacks can lead to demands for hefty ransom payments to restore access to encrypted systems and data. These attacks can also result in additional financial losses due to halted operations, decreased productivity, and revenue loss. Furthermore, the theft of sensitive information, such as financial records or proprietary data, can result in financial repercussions from fraud or intellectual property theft. The cost of recovering from a cyberattack can be significant. Recovery efforts often involve expenses related to forensic investigations, system repairs, and data restoration. Organizations may also incur costs associated with improving security measures to prevent future attacks. These costs can be substantial, especially for smaller agricultural businesses with limited resources. In addition, organizations may face legal and regulatory costs if they are found to have failed to protect sensitive information adequately. The combined financial burden of recovery and mitigation can have long-lasting effects on an organization's bottom line (Mattera *et al*., 2022).

Cybersecurity threats can severely disrupt supply chain processes within agriculture. For example, a cyberattack on an agricultural input supplier or processing facility can halt production and delay the delivery of essential products. Disruptions can cascade through the supply chain, affecting downstream activities such as distribution and retail (Ivanov, 2021). The inability to access critical systems or data can lead to operational inefficiencies, inventory shortages, and logistical challenges. Such disruptions can have a ripple effect on the entire supply chain, leading to broader implications for food security and market stability. Cyberattacks can cause significant delays in production and distribution processes (Pandey *et al*., 2020). For instance, if an attack targets automated farming equipment or processing machinery, it can result in operational shutdowns and delays in completing agricultural tasks. Similarly, attacks on distribution systems can disrupt the timely delivery of products to market. These delays can lead to a backlog of orders, increased costs, and potential losses in market share. The impact on production and distribution can ultimately affect the availability and pricing of agricultural products, influencing both consumer access and market dynamics.

One of the most damaging impacts of cybersecurity threats is the loss of consumer trust. When a cyberattack results in the exposure of sensitive information or disrupts supply chain operations, consumers may lose confidence in the affected organizations. This loss of trust can be particularly damaging in the agriculture sector, where transparency and reliability are crucial for consumer confidence (Lam *et al*., 2020). A breach that leads to compromised data or disrupted product availability can undermine the reputation of the affected company and erode consumer loyalty. The reputational damage resulting from cybersecurity threats can have long-term effects on a brand. A publicized cyberattack can damage the image of an organization, leading to negative media coverage and public perception. Rebuilding a damaged brand can be a challenging and costly process, often requiring significant investments in public

relations and marketing efforts. The long-term consequences of reputational damage can include decreased customer retention, reduced market competitiveness, and diminished business opportunities. Cybersecurity threats pose a significant risk to agriculture, with far-reaching impacts on economic stability, operational efficiency, and brand reputation. The financial losses resulting from cyberattacks, combined with the costs of recovery and mitigation, can be substantial. Operational disruptions and delays in production and distribution further exacerbate the challenges faced by agricultural businesses (Khan *et al*., 2022). Additionally, the loss of consumer trust and damage to brand reputation can have lasting effects on an organization's market position and consumer relationships. Addressing these impacts requires a proactive approach to cybersecurity, including robust protection measures, comprehensive risk management strategies, and ongoing vigilance to safeguard against evolving threats. By understanding and mitigating the impacts of cybersecurity threats, agricultural organizations can enhance their resilience and ensure the stability and sustainability of their operations in an increasingly digital world.

6. Mitigation Strategies and Best Practices

In the face of rising cybersecurity threats, implementing effective mitigation strategies and best practices is essential for safeguarding agriculture supply chains (Drape *et al*., 2021). These strategies encompass technological solutions, human-centric approaches, and policy and regulatory measures. A comprehensive approach combining these elements can significantly enhance security and resilience against cyber threats.

The foundation of a secure agriculture supply chain lies in implementing robust cybersecurity measures. This includes deploying firewalls, intrusion detection systems (IDS), and anti-malware software to protect against unauthorized access and malicious attacks. Network segmentation is another critical measure, as it limits the spread of cyber threats within the system (Djenna *et al*., 2021). For instance, separating critical control systems from general administrative networks can reduce the risk of a single breach compromising the entire network. Additionally, strong authentication mechanisms, such as multi-factor authentication (MFA), should be employed to ensure that only authorized personnel have access to sensitive systems and data. Keeping systems and software up-to-date is crucial for mitigating vulnerabilities. Regular updates and patch management help address known security flaws that cybercriminals could exploit. This includes applying security patches to operating systems, applications, and firmware for IoT devices. Automated patch management tools can assist in ensuring that updates are applied promptly and consistently across all systems. Regular updates are essential for protecting against emerging threats and vulnerabilities that could otherwise leave systems exposed to attacks (Newaz *et al*., 2021). Advanced technologies, such as artificial intelligence (AI) and machine learning (ML), offer significant advantages for threat detection and response. AI and ML algorithms can analyze vast amounts of data to identify unusual patterns and potential threats that might go unnoticed by traditional security measures. For example, machine learning models can detect anomalies in network traffic or user behavior, indicating possible security breaches or malicious activity. Implementing AI-driven security solutions can enhance the ability to detect, respond to, and mitigate cyber threats in real-time, providing an additional layer of protection for agriculture supply chains (Bechtsis *et al*., 2022).

Human factors are often a critical vulnerability in cybersecurity. Effective training and awareness programs are essential for educating employees about cybersecurity risks and best practices. Regular training sessions should cover topics such as recognizing phishing attempts, secure password practices, and proper handling of sensitive information. Awareness programs can also include simulated phishing exercises to test and reinforce employees' ability to identify and respond to cyber threats (Yeoh *et al* 2022). By enhancing employees' cybersecurity knowledge and skills, organizations can reduce the likelihood of successful attacks caused by human error. Building a strong culture of cybersecurity involves integrating security practices into the organization's daily operations and decision-making processes. This includes promoting a security-first mindset among all employees, encouraging proactive behavior, and fostering open communication about cybersecurity concerns. Leadership should prioritize cybersecurity and allocate resources to support security initiatives. Regular discussions about cybersecurity challenges and successes can help reinforce the importance of security and keep it at the forefront of organizational priorities (Loonam *et al*., 2020). Creating a culture of cybersecurity ensures that all members of the organization are engaged and committed to maintaining a secure environment.

Establishing and enforcing cybersecurity standards is crucial for ensuring a consistent and effective approach to security across the agriculture sector. Organizations should develop comprehensive cybersecurity policies that outline security requirements, responsibilities, and procedures (Mishra *et al*., 2022). These policies should align with industry standards and best practices, such as those provided by the National Institute of Standards and Technology (NIST) or the International Organization for Standardization (ISO). Regular audits and assessments can help ensure compliance with these standards and identify areas for improvement. By adhering to established standards, organizations can enhance their security posture and reduce the risk of cyber threats. Collaboration between government and private

sectors is vital for addressing cybersecurity challenges effectively. Governments can provide guidance, resources, and support for cybersecurity initiatives, while private sector organizations can contribute their expertise and technological advancements (Fadia *et al*., 2020). Public-private partnerships can facilitate information sharing about emerging threats, vulnerabilities, and best practices. Collaborative efforts can also lead to the development of industry-specific cybersecurity frameworks and standards that address the unique needs of sectors such as agriculture. By working together, both sectors can strengthen their collective defenses and improve overall resilience against cyber threats. Mitigating cybersecurity threats in agriculture supply chains requires a multifaceted approach that includes technological solutions, human-centric strategies, and policy and regulatory measures. Implementing robust cybersecurity measures, maintaining regular updates and patch management, and leveraging advanced technologies like AI and machine learning can enhance protection against cyber threats (Jimmy, 2021). Equally important are human-centric approaches, such as cybersecurity training and fostering a culture of security, which help address vulnerabilities arising from human factors. Additionally, developing and enforcing cybersecurity standards and promoting collaboration between government and private sectors are essential for creating a comprehensive and effective security framework. By adopting these strategies and best practices, agriculture supply chains can enhance their resilience and safeguard against the evolving landscape of cybersecurity threats.

7. Future Directions and Emerging Trends in Cybersecurity for Agriculture

As cybersecurity threats continue to evolve, the agriculture sector must adapt to emerging challenges and opportunities. Future directions and emerging trends in cybersecurity for agriculture focus on advances in technology, evolving policy and regulation, and the importance of continuous monitoring and adaptation (Araújo *et al*., 2021). These aspects will play a critical role in strengthening the resilience of agriculture supply chains against cyber threats.

The field of cybersecurity is witnessing rapid advancements in threat detection and response technologies. Innovations such as advanced machine learning algorithms and artificial intelligence (AI) are enhancing the ability to identify and mitigate cyber threats. AI-driven threat detection systems can analyze vast amounts of data in real time, recognizing patterns and anomalies that may indicate a security breach (Reddy, 2021). For example, AI can detect subtle changes in network traffic or user behavior that traditional methods might miss. Additionally, automated response systems powered by AI can rapidly contain and remediate threats, reducing the time and impact of security incidents. These advancements promise to improve the speed and accuracy of threat detection, offering more robust protection for agriculture supply chains. As technology evolves, new tools and techniques are being developed to enhance the security of agriculture supply chains. One notable trend is the integration of blockchain technology to improve transparency and traceability. Blockchain can provide a secure, immutable record of transactions and interactions within the supply chain, reducing the risk of tampering and fraud (Agarwal *et al*., 2022). Additionally, the adoption of zero trust architecture, which operates on the principle of never trusting and always verifying, is becoming more prevalent. Zero trust ensures that access to systems and data is continuously validated, minimizing the risk of unauthorized access. Other emerging tools include advanced encryption techniques, secure IoT protocols, and next-generation firewalls, all contributing to a more secure agricultural environment.

The regulatory landscape for cybersecurity is expected to evolve in response to growing threats and increasing awareness. Future regulations are likely to emphasize stricter requirements for data protection, incident reporting, and cybersecurity practices. Governments may introduce new standards and compliance mandates tailored to specific industries, including agriculture (Hamman *et al*., 2021). These changes will require organizations to enhance their cybersecurity measures and adopt more rigorous practices. For instance, regulations may mandate regular security assessments, mandatory encryption of sensitive data, and enhanced incident response protocols. Staying abreast of regulatory changes and ensuring compliance will be crucial for organizations to avoid legal repercussions and maintain a strong security posture (Garrett and Mitchell, 2020). International cooperation is becoming increasingly important in the fight against cyber threats. Global collaboration can lead to the development of unified cybersecurity standards, information sharing platforms, and joint response strategies. International partnerships, such as those facilitated by organizations like the International Organization for Standardization (ISO) and the Global Forum on Cyber Expertise (GFCE), are helping to align cybersecurity practices across borders (Roshanaei, 2021). These collaborations enable countries to share threat intelligence, best practices, and resources, enhancing the collective ability to combat cyber threats. For agriculture, international cooperation can lead to the adoption of consistent security frameworks and the exchange of critical information on emerging threats and vulnerabilities (Karie *et al*., 2021).

Continuous monitoring and risk assessment are essential for maintaining effective cybersecurity (Goel *et al*., 2020). The dynamic nature of cyber threats necessitates regular evaluation of security measures and risk profiles. Ongoing risk assessments help organizations identify new vulnerabilities, evaluate the effectiveness of existing controls, and adapt to changing threat landscapes. Implementing continuous monitoring systems, such as Security Information and Event

Management (SIEM) solutions, enables real-time tracking of network activity and potential threats (Hussein and Hamza, 2022). Regular audits and penetration testing further contribute to identifying and addressing weaknesses in the security posture. By adopting a proactive approach to risk management, organizations can stay ahead of emerging threats and minimize their impact. Cybersecurity strategies must be adaptable to address the evolving nature of cyber threats. As attackers develop new techniques and tools, organizations need to continuously update and refine their security practices (Mironeanu *et al*., 2021). This includes adopting adaptive threat detection mechanisms, implementing flexible incident response plans, and investing in emerging technologies. For example, incorporating threat intelligence feeds and machine learning models can enhance the ability to detect and respond to novel threats. Additionally, organizations should foster a culture of agility and innovation, encouraging continuous improvement and adaptation in their cybersecurity practices. By remaining adaptable, organizations can effectively counter new and sophisticated threats, ensuring the ongoing protection of agriculture supply chains. The future of cybersecurity in agriculture is shaped by advancements in technology, evolving regulations, and the necessity for continuous adaptation. Innovations in threat detection and response, such as AI and blockchain, promise to enhance security capabilities. Regulatory changes and international cooperation will further influence cybersecurity practices, driving the adoption of more stringent standards and collaborative efforts. Continuous monitoring and adaptive strategies are crucial for addressing the ever-changing threat landscape and ensuring the resilience of agriculture supply chains (Chisty *et al*., 2022). Embracing these future directions and trends will be essential for safeguarding against emerging cyber threats and maintaining robust security in the agriculture sector

8. Conclusion

Cybersecurity threats pose significant risks to agriculture supply chains, with impacts spanning economic, operational, and reputational domains. Cyberattacks, including malware, ransomware, phishing, and data breaches, can disrupt supply chain processes, lead to financial losses, and erode consumer trust. The vulnerabilities in agriculture supply chains are multifaceted, encompassing technological weaknesses, human factors, and systemic issues. Addressing these threats requires a comprehensive approach, integrating advanced technological solutions, human-centric strategies, and robust policy measures.

Mitigation strategies and best practices play a crucial role in enhancing the security of agriculture supply chains. Technological solutions, such as deploying advanced threat detection systems, implementing regular updates, and utilizing AI-driven tools, can significantly bolster defense mechanisms. Human-centric approaches, including cybersecurity training and fostering a culture of security, are vital in reducing vulnerabilities associated with human error. Additionally, developing and enforcing cybersecurity standards, along with promoting international collaboration, is essential for creating a unified and effective security framework.

The importance of proactive cybersecurity measures cannot be overstated. As cyber threats continue to evolve, adopting a proactive approach is crucial for safeguarding agriculture supply chains. Proactive measures include continuous risk assessment, adaptive security strategies, and the implementation of cutting-edge technologies. By prioritizing cybersecurity, stakeholders can not only protect against current threats but also anticipate and prepare for future challenges. Ensuring the resilience of agriculture supply chains requires ongoing vigilance, investment in security practices, and a commitment to maintaining a secure operational environment. Addressing cybersecurity threats in agriculture demands a multifaceted strategy encompassing technological advancements, human factors, and policy measures. Emphasizing a proactive approach and encouraging stakeholders to prioritize cybersecurity will be key to mitigating risks and ensuring the stability and security of agriculture supply chains in an increasingly digital world.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Agarwal, U., Rishiwal, V., Tanwar, S., Chaudhary, R., Sharma, G., Bokoro, P.N. and Sharma, R., 2022. Blockchain technology for secure supply chain management: A comprehensive review. *Ieee Access*, *10*, pp.85493-85517.

[2] Ahmad, A., Desouza, K.C., Maynard, S.B., Naseer, H. and Baskerville, R.L., 2020. How integration of cyber security management and incident response enables organizational learning. *Journal of the Association for Information Science and Technology*, *71*(8), pp.939-953.

[3] Araújo, S.O., Peres, R.S., Barata, J., Lidon, F. and Ramalho, J.C., 2021. Characterising the agriculture 4.0 landscape—emerging trends, challenges and opportunities. *Agronomy*, *11*(4), p.667.

[4] Asante, M., Epiphaniou, G., Maple, C., Al-Khateeb, H., Bottarelli, M. and Ghafoor, K.Z., 2021. Distributed ledger technologies in supply chain security management: A comprehensive survey. *IEEE Transactions on Engineering Management*, *70*(2), pp.713-739.

[5] Bahn, R.A., Yehya, A.A.K. and Zurayk, R., 2021. Digitalization for sustainable agri-food systems: potential, status, and risks for the MENA region. *Sustainability*, *13*(6), p.3223.

[6] Bechtsis, D., Tsolakis, N., Iakovou, E. and Vlachos, D., 2022. Data-driven secure, resilient and sustainable supply chains: gaps, opportunities, and a new generalised data sharing and data monetisation framework. *International Journal of Production Research*, *60*(14), pp.4397-4417.

[7] Borkovich, D.J. and Skovira, R.J., 2019. CYBERSECURITY INERTIA AND SOCIAL ENGINEERING: WHO'S WORSE, EMPLOYEES OR HACKERS?. *Issues in Information Systems*, *20*(3).

[8] Chisty, N.M.A., Baddam, P.R. and Amin, R., 2022. Strategic approaches to safeguarding the digital future: insights into next-generation cybersecurity. *Engineering International*, *10*(2), pp.69-84.

[9] Cremer, F., Sheehan, B., Fortmann, M., Kia, A.N., Mullins, M., Murphy, F. and Materne, S., 2022. Cyber risk and cybersecurity: a systematic review of data availability. *The Geneva papers on risk and insurance. Issues and practice*, *47*(3), p.698.

[10] Dey, K. and Shekhawat, U., 2021. Blockchain for sustainable e-agriculture: Literature review, architecture for data management, and implications. *Journal of Cleaner Production*, *316*, p.128254.

[11] Djenna, A., Harous, S. and Saidouni, D.E., 2021. Internet of things meet internet of threats: New concern cyber security issues of critical cyber infrastructure. *Applied Sciences*, *11*(10), p.4580.

[12] Drape, T., Magerkorth, N., Sen, A., Simpson, J., Seibel, M., Murch, R.S. and Duncan, S.E., 2021. Assessing the role of cyberbiosecurity in agriculture: A case study. *Frontiers in Bioengineering and Biotechnology*, *9*, p.737927.

[13] Etemadi, N., Borbon-Galvez, Y., Strozzi, F. and Etemadi, T., 2021. Supply chain disruption risk management with blockchain: A dynamic literature review. *Information*, *12*(2), p.70.

[14] Fadia, A., Nayfeh, M. and Noble, J., 2020. Follow the leaders: How governments can combat intensifying cybersecurity risks. *McKinsey & Company, September*, *16*.

[15] Garrett, B.L. and Mitchell, G., 2020. Testing compliance. *Law & Contemp. Probs.*, *83*, p.47.

[16] Goel, R., Kumar, A. and Haddow, J., 2020. PRISM: a strategic decision framework for cybersecurity risk assessment. *Information & Computer Security*, *28*(4), pp.591-625.

[17] Gupta, M., Abdelsalam, M., Khorsandroo, S. and Mittal, S., 2020. Security and privacy in smart farming: Challenges and opportunities. *IEEE access*, *8*, pp.34564-34584.

[18] Hamman, E., Deane, F., Kennedy, A., Huggins, A. and Nay, Z., 2021. Environmental regulation of agriculture in federal systems of government: The case of Australia. *Agronomy*, *11*(8), p.1478.

[19] Hartley, M.E., 2022. Access Denied: The Dangers of Ransomware's Unchecked Attack on the Agriculture Industry. *Drake J. Agric. L.*, *27*, p.457.

[20] Hazrati, M., Dara, R. and Kaur, J., 2022. On-farm data security: practical recommendations for securing farm data. *Frontiers in Sustainable Food Systems*, *6*, p.884187.

[21] Hussein, M.A. and Hamza, E.K., 2022. Secure Mechanism Applied to Big Data for IIoT by Using Security Event and Information Management System (SIEM). *International Journal of Intelligent Engineering & Systems*, *15*(6).

[22] Ivanov, D., 2021. Supply chain risks, disruptions, and ripple effect. In *Introduction to Supply Chain Resilience: Management, Modelling, Technology* (pp. 1-28). Cham: Springer International Publishing.

[23] Jagtap, S., Bader, F., Garcia-Garcia, G., Trollman, H., Fadiji, T. and Salonitis, K., 2020. Food logistics 4.0: Opportunities and challenges. *Logistics*, *5*(1), p.2.

[24] Jimmy, F., 2021. Emerging threats: The latest cybersecurity risks and the role of artificial intelligence in enhancing cybersecurity defenses. *Valley International Journal Digital Library*, pp.564-574.

[25] Kamilaris, A., Fonts, A. and Prenafeta-Boldú, F.X., 2019. The rise of blockchain technology in agriculture and food supply chains. *Trends in food science & technology*, *91*, pp.640-652.

[26] Karie, N.M., Sahri, N.M., Yang, W., Valli, C. and Kebande, V.R., 2021. A review of security standards and frameworks for IoT-based smart environments. *IEEE Access*, *9*, pp.121975-121995.

[27] Kayan, H., Nunes, M., Rana, O., Burnap, P. and Perera, C., 2022. Cybersecurity of industrial cyber-physical systems: A review. *ACM Computing Surveys (CSUR)*, *54*(11s), pp.1-35.

[28] Khan, S.A.R., Razzaq, A., Yu, Z., Shah, A., Sharif, A. and Janjua, L., 2022. Disruption in food supply chain and undernourishment challenges: An empirical study in the context of Asian countries. *Socio-Economic Planning Sciences*, *82*, p.101033.

[29] Kim, W.S., Lee, W.S. and Kim, Y.J., 2020. A review of the applications of the internet of things (IoT) for agricultural automation. *Journal of Biosystems Engineering*, *45*, pp.385-400.

[30] Kour, V.P. and Arora, S., 2020. Recent developments of the internet of things in agriculture: a survey. *Ieee Access*, *8*, pp.129924-129957.

[31] Kraft, S.K. and Kellner, F., 2022. Can blockchain be a basis to ensure transparency in an agricultural supply chain?. *Sustainability*, *14*(13), p.8044.

[32] Lam, T.K., Heales, J., Hartley, N. and Hodkinson, C., 2020. Consumer trust in food safety requires information transparency. *Australasian Journal of Information Systems*, *24*.

[33] Lang, E.L., 2022. Seven (Science-Based) commandments for understanding and countering insider threats. *Counter-Insider Threat Research and Practice*, *1*(1).

[34] Latino, M.E., Menegoli, M., Lazoi, M. and Corallo, A., 2022. Voluntary traceability in food supply chain: a framework leading its implementation in Agriculture 4.0. *Technological Forecasting and Social Change*, *178*, p.121564.

[35] Lehto, M., 2022. Cyber-attacks against critical infrastructure. In *Cyber security: Critical infrastructure protection* (pp. 3-42). Cham: Springer International Publishing.

[36] Loonam, J., Zwiegelaar, J., Kumar, V. and Booth, C., 2020. Cyber-resiliency for digital enterprises: a strategic leadership perspective. *IEEE Transactions on Engineering Management*, *69*(6), pp.3757-3770.

[37] Mattera, M., Alba Ruiz-Morales, C., Gava, L. and Soto, F., 2022. Sustainable business models to create sustainable competitive advantages: strategic approach to overcoming COVID-19 crisis and improve financial performance. *Competitiveness Review: An International Business Journal*, *32*(3), pp.455-474.

[38] Meemken, E.M., Barrett, C.B., Michelson, H.C., Qaim, M., Reardon, T. and Sellare, J., 2021. Sustainability standards in global agrifood supply chains. *Nature Food*, *2*(10), pp.758-765.

[39] Melnyk, S.A., Schoenherr, T., Speier-Pero, C., Peters, C., Chang, J.F. and Friday, D., 2022. New challenges in supply chain management: cybersecurity across the supply chain. *International Journal of Production Research*, *60*(1), pp.162-183.

[40] Mironeanu, C., Archip, A., Amarandei, C.M. and Craus, M., 2021. Experimental cyber attack detection framework. *Electronics*, *10*(14), p.1682.

[41] Mishra, A., Alzoubi, Y.I., Gill, A.Q. and Anwar, M.J., 2022. Cybersecurity enterprises policies: A comparative study. *Sensors*, *22*(2), p.538.

[42] Mousavi, S.K., Ghaffari, A., Besharat, S. and Afshari, H., 2021. Security of internet of things based on cryptographic algorithms: a survey. *Wireless Networks*, *27*(2), pp.1515-1555.

[43] Mugarza, I., Flores, J.L. and Montero, J.L., 2020. Security issues and software updates management in the industrial internet of things (iiot) era. *Sensors*, *20*(24), p.7160.

[44] Newaz, A.I., Sikder, A.K., Rahman, M.A. and Uluagac, A.S., 2021. A survey on security and privacy issues in modern healthcare systems: Attacks and defenses. *ACM Transactions on Computing for Healthcare*, *2*(3), pp.1-44.

[45] Obaidat, M.A., Obeidat, S., Holst, J., Al Hayajneh, A. and Brown, J., 2020. A comprehensive and systematic survey on the internet of things: Security and privacy challenges, security frameworks, enabling technologies, threats, vulnerabilities and countermeasures. *Computers*, *9*(2), p.44.

[46] Paciarotti, C. and Torregiani, F., 2021. The logistics of the short food supply chain: A literature review. *Sustainable Production and Consumption*, *26*, pp.428-442.

[47] Pandey, S., Singh, R.K., Gunasekaran, A. and Kaushik, A., 2020. Cyber security risks in globalized supply chains: conceptual framework. *Journal of Global Operations and Strategic Sourcing*, *13*(1), pp.103-128.

[48] Quayson, M., Bai, C. and Osei, V., 2020. Digital inclusion for resilient post-COVID-19 supply chains: Smallholder farmer perspectives. *IEEE Engineering Management Review*, *48*(3), pp.104-110.

[49] Reddy, A.R.P., 2021. The Role of Artificial Intelligence in Proactive Cyber Threat Detection In Cloud Environments. *NeuroQuantology*, *19*(12), pp.764-773.

[50] Roshanaei, M., 2021. Resilience at the core: critical infrastructure protection challenges, priorities and cybersecurity assessment strategies. *Journal of Computer and Communications*, *9*(8), pp.80-102.

[51] Rosline, G.J., Rani, P. and Gnana Rajesh, D., 2022. Comprehensive analysis on security threats prevalent in IoT-based smart farming systems. In *Ubiquitous Intelligent Systems: Proceedings of ICUIS 2021* (pp. 185-194). Springer Singapore.

[52] Sanjeevi, P., Prasanna, S., Siva Kumar, B., Gunasekaran, G., Alagiri, I. and Vijay Anand, R., 2020. Precision agriculture and farming using Internet of Things based on wireless sensor network. *Transactions on Emerging Telecommunications Technologies*, *31*(12), p.e3978.

[53] Sjah, T. and Zainuri, Z., 2020. Agricultural supply chain and food security. In *Zero Hunger* (pp. 79-88). Cham: Springer International Publishing.

[54] Stupina, A.A., Rozhkova, A.V., Olentsova, J.A. and Rozhkov, S.E., 2021, September. Digital technologies as a tool for improving the efficiency of the agricultural sector. In *IOP Conference Series: Earth and Environmental Science* (Vol. 839, No. 2, p. 022092). IOP Publishing.

[55] Sujatha, R., Prakash, G. and Jhanjhi, N.Z. eds., 2022. *Cyber Security Applications for Industry 4.0*. CRC Press.

[56] Tsai, F.M., Bui, T.D., Tseng, M.L., Ali, M.H., Lim, M.K. and Chiu, A.S., 2021. Sustainable supply chain management trends in world regions: A data-driven analysis. *Resources, Conservation and Recycling*, *167*, p.105421.

[57] Washo, A.H., 2021. An interdisciplinary view of social engineering: A call to action for research. *Computers in Human Behavior Reports*, *4*, p.100126.

[58] West, J., 2020. Advances in data security for more effective decision-making in agriculture. In *Improving data management and decision support systems in agriculture* (pp. 59-94). Burleigh Dodds Science Publishing.

[59] Yeoh, W., Huang, H., Lee, W.S., Al Jafari, F. and Mansson, R., 2022. Simulated phishing attack and embedded training campaign. *Journal of Computer Information Systems*, *62*(4), pp.802-821.