Cybersäkerhet i lantbruket

Digital sårbarhet och behov av stöd

Jakob Frisk

Examensarbete/Självständigt arbete • 15 hp
Sveriges lantbruksuniversitet, SLU
Fakulteten för Landskapsarkitektur, trädgårds- och växtproduktionsvetenskap
Institutionen för biosystem och teknologi
Lantmästarprogrammet
Alnarp 2026

Cybersäkerhet i lantbruket: Digital sårbarhet och behov av stöd

Cybersecurity in agriculture: Digital vulnerabilities and the need for support

Jakob Frisk

Handledare:	**Oleksiy Guzhva, Sveriges Lantbruksuniversitet, Institutionen för biosystem och teknologi**
Bitr. handledare:	Martin Svärd, Hushållningssällskapet, Nationell-IT
Examinator:	Daniel Nilsson, Sveriges Lantbruksuniversitet, Institutionen för biosystem och teknologi

Omfattning:	15 hp
Nivå och fördjupning:	Grundnivå, G2E
Kurstitel:	Självständigt arbete i Lantbruksvetenskap, G2E - Lantmästarprogrammet
Kurskod:	EX1017
Program/utbildning:	Lantmästarprogrammet
Kursansvarig inst.:	Institutionen för biosystem och teknologi
Utgivningsort:	Alnarp
Utgivningsår:	2026
Omslagsbild:	OpenAI. (2026). Cybersäkerhet inom lantbruket [AI-genererad bild]. DALL·E. http://chat.openai.com/
Upphovsrätt:	Alla bilder används med upphovspersonens tillstånd.
Nyckelord:	cybersäkerhet, digitalisering, informationssäkerhet, lantbruk, riskuppfattning

Sveriges lantbruksuniversitet
Fakulteten för Landskapsarkitektur, trädgårds-och växtproduktionsvetenskap
Institutionen för biosystem och teknologi

Sammanfattning

Lantbruket har under senare år blivit mer beroende av uppkopplade och datadrivna system. Teknik som GPS-styrning, sensorer, stallautomation och fjärrsupport skapar möjligheter till ökad effektivitet, bättre beslutsunderlag och förbättrad arbetsmiljö. Samtidigt innebär denna utveckling ett beroende av fungerande nätverk, leverantörssystem och grundläggande cybersäkerhetsrutiner. Syftet med denna studie är att undersöka i vilken utsträckning svenska lantbrukare använder de digitala systemen, hur deras arbete med cybersäkerhet ser ut, hur de uppfattar risker och vilket stöd de efterfrågar för att minska sårbarheten. Studien bygger på en kombination av litteraturöversikt och en kvantitativ enkät.

Resultatet visar att de studerade gårdarna i hög grad är digitaliserade, men att de grundläggande cybersäkerhetsåtgärderna inte tillämpas tillräckligt. Regelbunden säkerhetskopiering är begränsad, användning av unika lösenord och tvåfaktorautentisering är låg, få har separata nätverk och de flesta saknar en plan för hur IT-relaterade incidenter ska hanteras. Samtidigt är phishing och driftstörningar i leverantörstjänster relativt vanligt förekommande. Respondenterna uppvisar en förhållandevis låg riskuppfattning gällande den egna gården som potentiellt mål för cyberangrepp, trots att många bedömer att konsekvenserna av ett större systemavbrott skulle kunna bli allvarliga. Ett tydligt stödbehov identifieras, särskilt kring rutiner vid en incident, säkerhetskopiering, kontoskydd och nätverkssäkerhet. Checklista, rådgivning och kortare utbildningsinsatser efterfrågas mer än andra stöd och utbildningsformer.

Cybersäkerhet i lantbruket bör ses som en socioteknisk fråga. Sårbarheten uppstår inte enbart på grund av tekniken, utan genom samspelet mellan teknik, användarbeteende, organisatoriska rutiner och externa beroenden till leverantörer och support. Lantbrukets digitalisering har gått snabbare än utvecklingen av dess grundläggande cybersäkerhetsrutiner. För att minska sårbarheten behövs verksamhetsnära, målgruppsanpassat och praktiskt stöd som gör det lättare för lantbrukare att genomföra enkla men effektiva säkerhetsåtgärder.

Nyckelord: cybersäkerhet, digitalisering, informationssäkerhet, lantbruk, riskuppfattning

Abstract

Agriculture has in recent years become increasingly dependent on connected and data-driven systems. Technologies such as GPS guidance, sensors, barn automation, and remote support create opportunities for increased efficiency, better decision-making, and improved working conditions. At the same time, this development entails a growing dependence on functioning networks, supplier systems, and basic cybersecurity routines. The purpose of this study is to investigate the extent to which Swedish farmers use digital systems, how they work with cybersecurity, how they perceive risks, and what kind of support they request to reduce vulnerability. The study is based on a combination of a literature review and a quantitative survey.

The result show that the farms studied are highly digitalized, but that basic cybersecurity measures are not applied sufficiently. Regular backups are limited, the use of unique passwords and two-factor authentication is low, few farms have separate networks, and most lack a plan for handling IT-related incidents. At the same time, phishing and service disruptions in supplier systems are relatively common. Respondents demonstrate a relatively low perception of risk regarding their own farms as potential targets of cyberattacks, despite many assessing that the consequences of a major system outage could be severe. A clear need for support is identified, particularly regarding incident response routines, backups, account protection and network security. Checklists, advisory services, and shorter training initiatives are requested more often than other forms of support and education.

Cybersecurity in agriculture should be viewed as a sociotechnical issue. Vulnerability does not arise solely because of the technology itself, but through the interaction between technology, user behavior, organizational routines, and external dependencies on suppliers and support services. The digitalization of agriculture has progressed faster than the development of its basic cybersecurity routines. To reduce vulnerability, there is a need for practical, target-group-adapted, and operational support that makes it easier for farmers to implement simple but effective security measures.

Keywords: cybersecurity, digitalization, information security, agriculture, risk perception

Förord

Lantmästarprogrammet är en treårig utbildning vid Sveriges lantbruksuniversitet i Alnarp, motsvarande 180 hp. Som avslutande moment genomförs ett självständigt arbete som redovisas både skriftligt och muntligt i form av ett seminarium. Det självständiga arbetet motsvarar 15 hp, och genomförs under en arbetsperiod som motsvarar cirka tio veckors heltidsstudier.

Under min uppväxt på en gård, samt utifrån tidigare arbetslivserfarenhet har jag sett hur verksamheten succesivt har blivit allt mer beroende av digital teknik, där till exempel maskinstyrning, övervakningssystem och olika typer av sensorer har blivit en naturlig del av det dagliga arbetet. Samtidigt som denna utveckling har bidragit till ökad effektivitet och bättre beslutsunderlag, har det också medfört risker som inte alltid uppmärksammas. Jag har upplevt att frågor kring cybersäkerhet sällan diskuteras i praktiken, trots att många system är uppkopplade och potentiellt sårbara.

Jag vill med detta arbete belysa hur lantbrukare förhåller sig till digitala säkerhetsrisker samt vilket behov som finns av ökad kunskap och stöd inom området. Förhoppningen är att studien kan bidra till en ökad medvetenhet och fungera som ett underlag för framtida rådgivning och utbildning.

Stort tack till Hushållningssällskapet som kom med idén till studien, samt stöttning under studiens gång. Jag vill rikta ett stort tack till de lantbrukare som tagit sig tid att delta i enkätstudien och därmed gjort detta arbete möjligt. Ett tack riktas även till handledare och övriga personer som bidragit med värdefulla synpunkter under arbetets gång.

Alnarp, Maj 2026

Jakob Frisk

Innehållsförteckning

Tabellförteckning

Figurförteckning

Förkortningar

Förkortning	Betydelse	Förklaring
AI	Artificiell Intelligens	Datorer som lär sig och fattar beslut.
CIA	Confidentiality, Integrity, Availability	Säkerhetens tre grundprinciper.
DDos	Distributed denial of service	Många enheter överbelastar en tjänst.
Dos	Denial of service	Överbelastning som stoppar en tjänst.
IT	Information Technology	Hantering av digital information.
IoT	Internet of Things	Uppkopplade enheter som kommunicerar.
MITM	Man in the middle	Avlyssning av kommunikation.
OT	Operational Technology	Styrning av maskiner och processer.
2FA	Tvåfaktorautentisering	Inloggning med två säkerhetssteg.

1. Inledning

1.1 Bakgrund

Jordbrukssektorn genomgår just nu en omfattande digital transformation som kännetecknas av implementering av tekniska hjälpmedel som IoT (Internet of Things), precisionsjordbrukssystem, autonoma maskiner samt avancerade dataanalysplattformar (Alahe et al. 2024). Denna utveckling, ofta kallad Agriculture 4.0/Jordbruk 4.0 eller smart jordbruk, förväntas medföra betydande förbättringar gällande skördeutbyte, resurseffektivitet, miljömässig hållbarhet och operativt beslutfattande (Alahe et al. 2024). Det skapar förutsättningar för datadrivna åtgärder som optimerar produktiviteten samtidigt som resursförbrukning och svinn minimeras (Gupta et al. 2020).

Integrationen av sammankopplade digitala system i jordbruksverksamheter har dock medfört betydande cybersäkerhetsrelaterade sårbarheter som hotar integriteten, tillgängligheten och konfidentialiteten (CIA-triaden) hos kritisk infrastruktur för jordbruket. Jordbrukssektorns ökade beroende av teknik har gjort den mer mottaglig för cyberhot, med potentiella konsekvenser som sträcker sig bortom enskilda gårdar och omfattar regional livsmedelssäkerhet, ekonomisk stabilitet samt konsumenters förtroende (Adewusi et al. 2022).

Till skillnad från andra sektorer, där etablerade cybersäkerhetsrutiner ofta finns på plats, så står jordbruket inför särskilda utmaningar kopplade till geografiskt spridda verksamheter, resursbegränsade enheter, begränsad teknisk kompetens hos användare samt integrationen av äldre system med modern digital infrastruktur (Angyalos et al. 2021; Kristen et al. 2021).

IoT har blivit en grundläggande del av teknologin bakom agriculture 4.0 och 5.0, och möjliggör realtidsinsamling av data för precisionsodling och djurhälsa (Maraveas et al. 2024). Dock visar forskning att införandet av IoT har breddat attackytan i jordbruket och därmed ökat sektorns sårbarhet. Den ökade sammankopplingen mellan IT (Information Technology)- och OT (Operational Technology) -miljöer skapar fler åtkomstpunkter, vilket gör det lättare för angripare att tränga in i produktionssystem (Kristen et al. 2021).

Cyberattacker mot aktörer inom livsmedelssektorn i Sverige har tydligt visat hur sårbart det kan vara. Ett exempel är händelsen 2022 där Lantmännen upptäckte och avvärjde en planerad cyberattack, vilket ledde till att delar av IT-miljön stängdes ned i förebyggande syfte. Verksamheten kunde upprätthållas tack vare alternativa processer (Lantmännen 2022). Denna typ av incidenter visar hur cyberangrepp inte

bara kan påverka en enskild organisation, utan även få konsekvenser för hela försörjningskedjan. Det understryker behovet av robusta cybersäkerhetsstrategier för att minska riskerna.

Samtidigt framträder en tydlig svensk utvecklingslinje där digitalisering betraktas som ett medel för att stärka både konkurrenskraft och hållbarhet i jordbruket. Jordbruksverkets förstudie om ett kunskapsnav för digitaliserat jordbruk konstaterar att det finns ett kunskapsglapp och att primärproducenter behöver få bättre stöd i en allt mer komplex digital miljö (Tunberg et al. 2022).

1.2 Problembeskrivning

Digitaliseringen av lantbruket ökar snabbt, maskinstyrning, fjärrövervakning, sensorer och digitala system innebär både möjligheter och risker. Denna utveckling innebär att lantbruket i allt högre grad exponeras för cybersäkerhetsrisker.

Tidigare forskning har visat att bristande säkerhetsmedvetenhet gör sektorn särskilt sårbar för cyberangrepp (Adewusi et al. 2022), samtidigt som begränsade resurser och budgetrestriktioner försvårar implementeringen av robusta säkerhetsåtgärder (Angyalos et al. 2021; Neethirajan 2025). Trots detta är kunskapen begränsad kring hur lantbrukare uppfattar och hanterar dessa risker. Det finns därmed en kunskapslucka kring hur cybersäkerhet faktiskt hanteras på gårdsnivå, samt vilket behov som finns av stöd, rådgivning och utbildning.

1.3 Mål, syfte och frågeställning

Syftet med studien är att undersöka hur medvetna lantbrukare är om digitala säkerhetsrisker, hur skyddet ser ut i praktiken och vilket behov som finns av rådgivning eller utbildning kring cybersäkerhet för att minska den digitala sårbarheten. Arbetets utgångspunkt är att lantbrukets digitalisering har gått snabbare än utvecklingen av motsvarande säkerhetsrutiner, och att den centrala sårbarheten därför är socioteknisk och inte enbart teknisk. Sårbarheten uppstår i samspel mellan digital teknik, mänskligt beteende och organisatoriska rutiner.

Litteraturgenomgången ger en översikt av de cybersäkerhetutmaningar som finns inom lantbruket, genom att sammanfatta forskning om hot, sårbarheter, skyddsåtgärder och behov av stöd. Utifrån de kunskapsluckor som identifierats bidrar denna studie till att, med hjälp av en kvantitativ enkät, undersöka hur lantbrukare ser på och arbetar med cybersäkerhet i praktiken. Genom att analysera enkätresultaten är målet att bidra med kunskap som kan användas för att ta fram

enkla effektiva och hållbara lösningar som både skyddar lantbrukets digitala system och stödjer fortsatt utveckling och digitalisering.

Frågeställningen för studien lyder: Hur förhåller sig lantbrukare till de digitala säkerhetsriskerna och hur stort är behovet av ökat stöd och kunskap i området?

1.4 Avgränsning

Studien är avgränsad till att fokusera på gårdar med primärproduktion i Sverige. Avsikten är att analysera cybersäkerheten kopplat till gårdens digitala system, inte övriga delar av produktionskedjan, även om dessa kan vara relevanta i en omvärlds- och beroendekontext.

Med digitala system avses både administrativ IT, verksamhetsstöd och operativ teknik som direkt påverkar fysiska processer på gården (t.ex. ventilation, utfodring, mjölknings- och grindstyrning, bevattning och maskinstyrning).

Studien syftar inte till att göra en teknisk undersökning och riskanalys, utan till att undersöka upplevd sårbarhet, faktiska grundrutiner och praktiska lösningar för stöd.

2. Material och metod

Denna studie är empirisk och bygger på information från vetenskapliga artiklar och rapporter. Datainsamlingen sker genom en kvantitativ enkätstudie. Studien har en deskriptiv och explorativ ansats. Studien fokuserar främst på att identifiera mönster, uppfattningar och praktiska erfarenheter. Metodvalet gjordes för att både skapa en teoretisk förståelse inom ämnet och samtidigt undersöka hur svenska lantbrukare arbetar med frågan i praktiken.

2.1 Litteraturgenomgång

Den litteratur som använts består främst av vetenskapliga publikationer och rapporter, samt i viss mån information från webbsidor. För att hitta relevant litteratur har databaser och verktyg som SLU Primo, ScienceDirect, Google Scholar, Asta AI samt Scispace använts.

Sökord som användes var bland annat: cybersecurity in agriculture, smart farming cybersecurity, agriculture 4.0, IoT security agriculture, digitalisering lantbruk, cybersäkerhet lantbruk.

2.2 Enkätstudie

Enkätstudien utgör studiens huvudsakliga datainsamlingsmetod och syftar till att undersöka lantbrukares uppfattningar och praktiska arbete med cybersäkerhet.

2.2.1 Målpopulation

Enkäten skickas ut till flera grupper på sociala medier för att nå en så stor, men relevant publik som möjligt. Målpopulationen utgörs av personer verksamma inom svensk primärproduktion i lantbruket. För att kunna besvara frågorna krävdes det att respondenten hade viss insyn i gårdens verksamhet.

2.2.2 Enkätens upplägg

Enkäten utformades med utgångspunkt i studiens syfte, tidigare forskning samt det sociotekniska perspektivet som används i arbetets teoretiska ramverk. Frågorna är gjorda för att fånga både de tekniska, organisatoriska och mänskliga samt externa aspekterna av cybersäkerheten.

Frågorna till enkäten finns som bilaga (bilaga 1). Frågorna är uppdelade i fyra olika kategorier, där den första delen har som syfte att identifiera gårdsprofilen. Del två handlar om att kartlägga gårdens digitala system och uppkoppling. Del tre belyser vilka skyddsåtgärder som lantbrukaren faktiskt har i praktiken. Den sista delen undersöker vilka typer av incidenter och erfarenheter som lantbrukaren har kopplat till cybersäkerhet i lantbruket.

2.2.3 Urval, utskick, svarsfrekvens, analys

Urvalet i studien är ett icke-slumpmässigt urval i form av ett så kallat bekvämlighetsurval (ett urval av lättåtkomliga deltagare), där respondenter rekryteras via relevanta grupper på sociala medier med inriktning på lantbruk och spannmålsodling.

Enkäten skapades i Netigate, ett webbaserat enkätverktyg för utformning, distribution och insamling av enkätdata. Datainsamlingen gjordes under tidsperioden 2026-04-17 till 2026-05-07. Totalt kom det in 65 svar, varav 52 fullständiga som kunde inkluderas i analysen.

2.2.4 Databearbetning och analys

Resultatet sammanställdes med hjälp av deskriptiv statistik. Analysen genomfördes utifrån studiens sociotekniska perspektiv och strukturerades enligt de tre analytiska dimensioner som beskrivs i avsnitt 3.1.3.

3. Litteraturstudie

3.1 Teoretisk ram

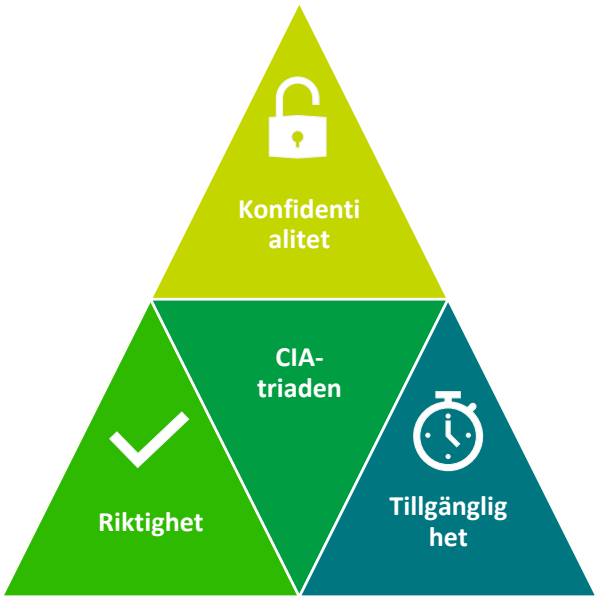
I detta kapitel presenteras de teoretiska utgångpunkter som ligger till grund för analysen av cybersäkerheten i lantbruket. I takt med att lantbruket genomgår en omfattande digital transformation där uppkopplade system, automatisering och datadrivna beslut blir allt vanligare, så uppstår också nya typer av sårbarheter och risker kopplade till cybersäkerhet. Det teoretiska ramverket belyser både tekniska och organisatoriska perspektiv genom att kombinera etablerade teorier inom IT med forskning inom cybersäkerhet och digitalisering inom lantbruket, och på så sätt skapa en analytisk grund för att förstå hur cybersäkerhetsrisker uppstår, hanteras och påverkar verksamheten.

3.1.1 Cybersäkerhet – centrala begrepp

Studien utgår från att informations- och cybersäkerhet kan analyseras genom tre grundläggande skyddsintressen: konfidentialitet, riktighet och tillgänglighet.

Warkentin och Orgeron (2020) skriver att ”The goal of managing information security is to ensure the confidentiality, integrity and availability of valuable information assets that may be strategic, protected, sensitive, or proprietary”, vilket kan beskrivas med hjälp av CIA-triaden, illustrerat i Figur 1 (CIA-Triad 2024).

CIA står i detta fall för confidentiality (konfidentialitet), integrity (riktighet) och availability (tillgänglighet). Det är de tre principerna för informationssäkerhet som skyddar din information och data (CIA-Triad 2024). Konfidentialitet innebär att data skyddas mot obehörig åtkomst, integritet syftar till att säkerställa att data förblir korrekt och skyddad mot oönskade förändringar, medan tillgänglighet avser att behöriga användare och system kan få åtkomst till informationen när den behövs och i rätt format (Warkentin & Orgeron 2020).



Figur 1. CIA-triaden. (CIA-Triad 2024)

Exempelvis kan brister i säkerhetskopiering kopplas till tillgänglighet, medan svaga lösenord påverkar konfidentialitet. Genom att tolka enkätresultaten utifrån dessa dimensioner möjliggörs en strukturerad analys av var de största sårbarheterna finns.

Samma tredelning används i svensk incidentrapportering som ett sätt att beskriva hur en oönskad händelse påverkar ett system (MSB u.å.).

3.1.2 Sociotekniskt perspektiv

I denna studie analyseras cybersäkerhet utifrån ett sociotekniskt perspektiv, vilket innebär att både tekniska och mänskliga faktorer inkluderas. Användarbeteende, kunskapsnivå och organisatoriska rutiner spelar en avgörande roll för säkerhetsnivån. En bristande säkerhetsmedvetenhet kan innebära att de skyddsåtgärder som finns kringgås eller används felaktigt.

Rijswijk et al. (2021) beskriver digitalt jordbruk som ett socio-cyber-fysiskt system, medan Lundström och Lindblom (2018) visar att digitala beslutsstöd och automatiserade system måste passa lantbrukarens sociotekniska praktik för att bli meningsfulla och användbara.

Genom att inkludera detta perspektiv görs en mer heltäckande analys av cybersäkerheten i lantbruket, där samspel mellan människa, teknik och organisation står i fokus. Det sociotekniska perspektivet är en viktig teori för denna studie eftersom det belyser att cybersäkerhet i lantbruket uppstår i samspelet mellan teknik och människor.

3.1.3 Tre dimensioner

Analysen görs utifrån tre dimensioner: 1) tekniska, 2) organisatoriska och mänskliga, samt 3) externa beroenden och stödbehov. Den första dimensionen handlar om tekniknivån, och vilka digitala system som används och hur viktiga de är för verksamheten och vilka skydd samt backuplösningar som finns. Den andra handlar om människans och organisationens kunskap, säkerhetstänk och hur man upplever att man klarar av säkerhetsarbetet. Den tredje dimensionen belyser det externa stödet och hjälp utifrån, tillexempel från leverantörer, rådgivare och myndigheter.

Modellen bygger på ett sociotekniskt perspektiv där cybersäkerhet är ett resultat av samspelet mellan teknik, människan och organisationer. Den tekniska dimensionen relaterar främst till CIA-triadens aspekter av tillgänglighet och integritet, medan den organisatoriska och mänskliga dimensionen är nära kopplad till

användarbeteende och säkerhetsmedvetenhet. Den externa dimensionen belyser beroenden till aktörer utanför den egna verksamheten, såsom leverantörer och rådgivning.

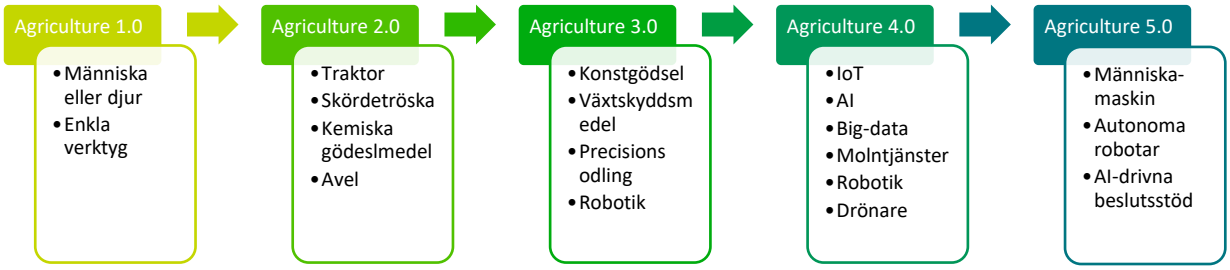
Denna modell ligger till grund för analyskapitlet, där resultaten från enkätstudien tolkas utifrån de tre dimensionerna.

3.2 Digitaliseringen inom lantbruket

3.2.1 Lantbrukets utveckling – 1.0 till 4.0

Lantbruket har haft en historisk progression från manuellt jordbruk (1.0) via mekanisering (2.0) och tidig precisionsodling (3.0) till fullt digitaliserade, data-intensiva system (4.0), där utvecklingen går mot en jordbruksmodell som integrerar avancerad AI, robotik och IoT för att möjliggöra ett datadrivet, effektivt och människocentrerat lantbruk (se Figur 2) (Saiz-Rubio & Rovira-Más 2020; Alahe et al. 2024; Goldenits & Neubauer 2025).

Just nu befinner vi oss i Agriculture 4.0, vilket beskrivs som ”smart farming” där IoT, AI, big-data, molntjänster, robotik och drönare integreras för realtidsövervakning, data-driven beslutsfattning och automatiserade processer. Målet är ökad effektivitet, hållbarhet och livsmedelssäkerhet, men det medför också en ökad cyber-sårbarhet (Alahe et al. 2024; Campoverde-Molina & Luján-Mora 2025).



Figur 2. Beskrivning av de olika jordbruksrevolutionerna. Idag befinner vi oss i 4.0, men variationen mellan olika gårdar är stor. (Egen bearbetning baserad på Saiz-Rubio & Rovira-Más 2020; Alahe et al. 2024; Goldenits & Neubauer 2025)

3.2.2 Hot, sårbarheter och konkreta exempel

Lantbrukare utgör den första ”försvarslinjen” för cybersäkerhet i lantbruket, men många saknar nödvändig utbildning i digitala säkerhetsrutiner. Forskning pekar konsekvent på att bristande cybersäkerhetsmedvetenhet är en betydande sårbarhet i jordbrukssystem (Adewusi et al. 2022).

Som tidigare nämnts visar händelsen hos Lantmännen att även aktörer i Sverige kan utsättas för cyberhot. Internationella exempel visar dock att konsekvenserna i vissa fall kan bli betydligt mer omfattande.

Ett uppmärksammat fall inträffade år 2021 då köttproducenten JBS Foods utsattes för en ransomwareattack. JBS är en av världen största köttproducenter och attacken ledde till omfattande störningar för verksamheten i Nordamerika och Australien. Flera anläggningar fick stoppa produktionen medans systemen återställdes (BBC 2021). Angreppet fick stor uppmärksamhet eftersom det visade att cyberattacker kan få konsekvenser i hela kedjan.

Cyberhot kan även få direkta konsekvenser på gårdsnivå. Ett annat uppmärksammat exempel är den schweiziske mjölkbonden som utsattes för en ransomwareattack mot den dator som var kopplad till gårdens mjölkningsrobot. Angriparna krypterade systemets data och krävde lösensumma för att återställa informationen. Mjölkningsroboten fortsatta fungera, men lantbrukaren förlorade tillgången till information om djurens hälsa och reproduktion. Det resulterade i komplikationer hos en dräktig ko, vilket ledde till att kalven dog i livmodern och kon behövde avlivas (Berchtold 2024).

Kristen et al. (2021) har identifierat tre huvudsakliga grupper av angreppsmotiv: spionage, förstörelser och sabotage som visas i Tabell 1.

Tabell 1. Tre grupper av angreppsmotiv

Spionage	Förstörelse och utpressning	Sabotage och missbruk
Obehörig åtkomst till data	Fysisk skada på jordbruksutrustning	Minskad tillgänglighet till jordbruksutrustning
Dataläckage	Försämrad produktkvalitet	Produktionsbortfall
Förlust av produktionsdata	Ransomware (utpressningsprogram)	Försämrad produktkvalitet
Nätfiske (phishing)	Datamanipulation	Botnät
Trojaner	Datadestruktion	DDos
IP stöld		MITM
Spionprgram (spyware)		

Källa: Kristen et al. 2021

Flera studier beskriver hur angripare kan stjäla känsliga produktionsdata genom oauktoriserad åtkomst till IoT-enheter, molntjänster eller interna nätverk (Kristen et al. 2021).

Ransomwareattacker innebär att angripare krypterar kritiska data eller låser och gör centrala system otillgängliga tills dess att en lösensumma betalats. Sådana angrepp sker ofta genom att sårbarheter utnyttjas, till exempel genom nätfiske (phishing) eller manipulerade programuppdateringar (Neethirajan 2025). Konsekvenserna kan bli omfattande driftstörningar, såsom att mjölkningssystem stannar eller schemalagd utfodring inte kan genomföras.

DoS- och DDoS-attacker överbelastar nätverk och på så sätt försämrar funktionaliteten. DoS (Denial of service) är en attack där en enskild dator används för att överbelasta en målenhet genom att skicka en stor mängd falsk trafik. DDoS (Distributed denial of service) liknar Dos, men attacken genomförs av ett samordnat kluster av datorer (Kristen et al. 2021).

Malware-familjer (trojaner, botnät, spyware) sprids via phishing-epost och manipulerade uppdateringar, vilket kan ge angripare kontroll över gårdens kritiska system (Kristen et al. 2021).

Fysiskt sabotage kan göra att utrustning utsätts för cyberattacker. Det kan vara att utrustning, t.ex. sensorer eller drönare, stjäls för att installera skadlig programvara på (Maraveas et al. 2024). De flesta tillämpningarna inom smart jordbruk idag är baserade på IoT teknologi, vilket kan medföra säkerhetsrisker i form av fysisk manipulation av enheter (Alahe et al. 2024).

Jordbrukets leveranskedjor är komplexa sammanlänkade system, från produktion och bearbetning till distribution och detaljhandel. Detta gör att det skapas flera tänkbara ingångspunkter för cyberangrepp som hotar hela leveranskedjans integritet (Adewusi et al. 2022). Dessa attacker kan vara riktade mot till exempel programuppdateringar för maskiner, tredjepartleverantörer eller olika logistiksamordningar eller leverantörsnätverk (Olateju 2025).

Sammantaget visar materialet att dataintrång, ransomware och olika former av driftstörningar, från nätverks till fysiska sabotage, är centrala risker för det moderna smarta jordbruket.

3.2.3 AI och cybersäkerhet

Utvecklingen av nya AI-modeller kan innebära en stor cybersäkerhetsrisk, men det kan också möjliggöra identifiering av svagheter och en förbättrad säkerhet.

Den 7 april 2026 presenterade Anthropic en experimentell AI-modell som är specialiserad på cybersäkerhet och avancerad analys (Anthropic 2026; Carlini et al. 2026).

Denna AI-modell kan hitta tidigare okända säkerhetsbrister och bygga fungerande attacker för att utnyttja dem. Detta gör modellen självständigt och det kan göras av användare utan djup teknisk kunskap.

Det innebär ett skifte där cyberattacker går från att vara manuella och ta tid, till att bli automatiserade, snabbare och mer tillgängliga. Att AI kan hitta och utnyttja sårbarheter i stor skala gör att system som tidigare ansågs säkra inte håller måttet.

3.3 Sammanfattning litteratur

Litteraturen pekar på två kunskapsluckor som är relevanta för detta arbete. För det första finns relativt få studier som undersöker cybersäkerhet på gårdsnivå med fokus på lantbrukares egna erfarenhet. För det andra är svenska data på området begränsad, trots att svenska myndigheter samtidigt efterfrågar bättre kunskapsstöd kring digitaliseringens praktiska konsekvenser.

4. Resultat

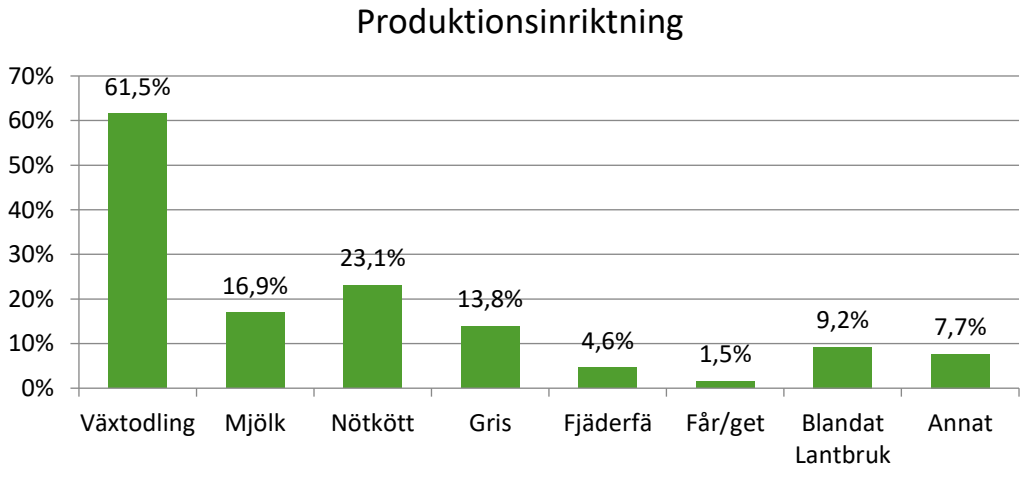
Resultaten presenteras utifrån studiens tre analytiska dimensioner: tekniska system och skyddsåtgärder, organisatoriska och mänskliga faktorer samt externa beroenden och stödbehov.

4.1 Resultat från enkätstudien

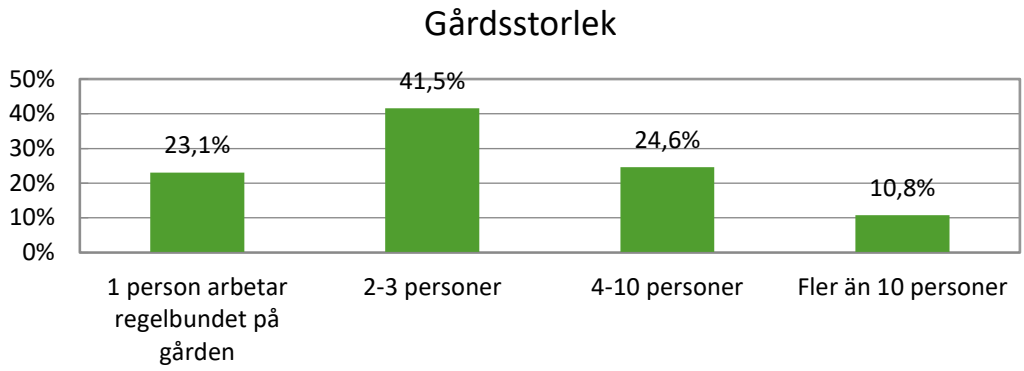
Svarsfrekvensen på enkäten var 65, varav 52 var fullständiga och inkluderades i resultatet och analysen. Enkäten har publicerats på sociala medier i grupper med inriktning lantbruk och spannmålsodling.

4.1.1 Respondentprofil och gårdsprofil

Majoriteten av respondenterna bedriver växtodling (62 %), vilket innebär att resultaten främst speglar denna typ av produktion (se Figur 3). Detta kan påverka vilka cybersäkerhetsrisker som identifieras, då växtodling ofta är mindre beroende av realtidsstyrda system än exempelvis mjölkproduktion. Den höga andelen växtodling beror också på att totalt 41 respondenter hade både växtodling och någon annan typ av produktion på gården. Kategorin ”Annat” innefattar bland annat maskinstation och grönsaksodling.

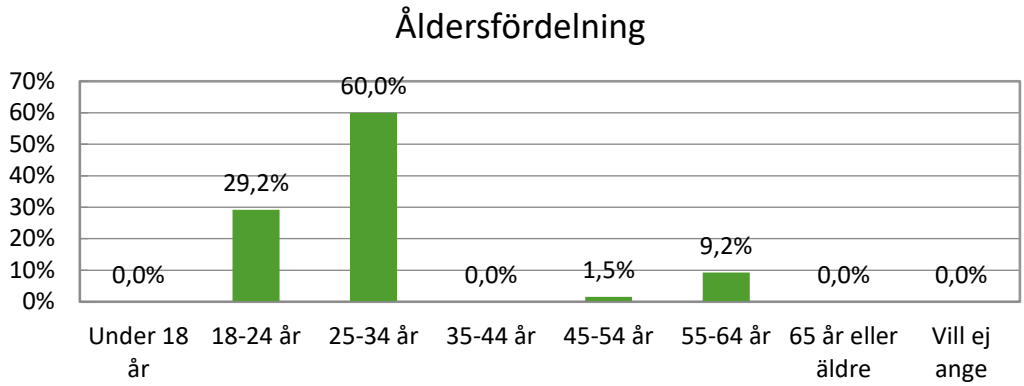


Figur 3. Fördelning av produktionsinriktning bland respondenter.



Figur 4. Gårdsstorlek baserat på antal personer i verksamheten.

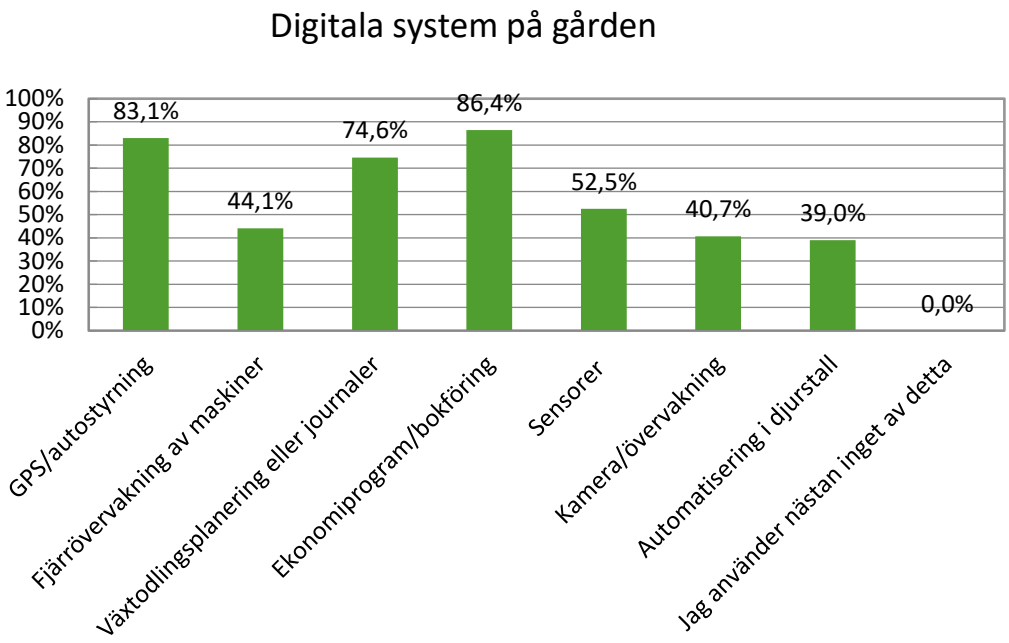
Den vanligaste gårdsstorleken har 2–3 personer som arbetar regelbundet på gården (se Figur 4). Resultaten speglar därmed främst små till medelstora lantbruksföretag med relativt hög användning av digitala system.



Figur 5. Åldersfördelning bland respondenter

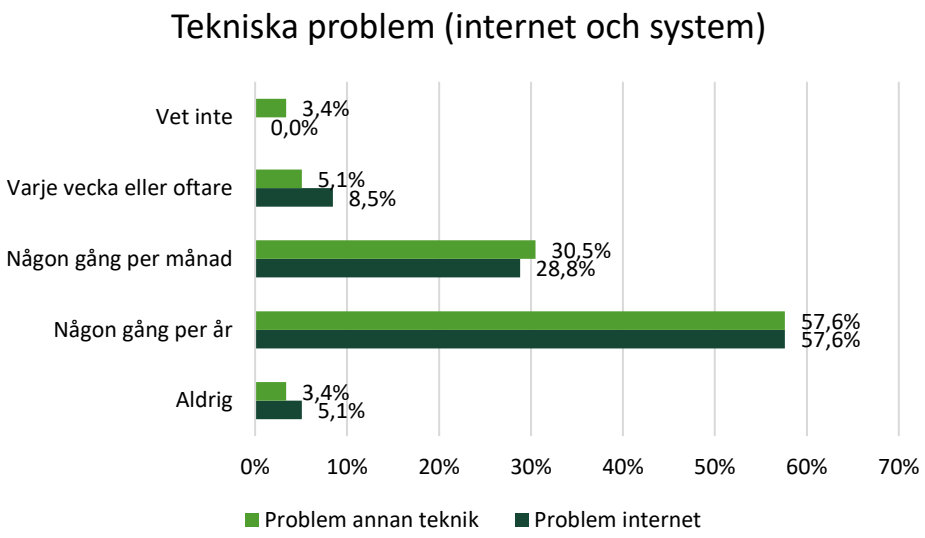
Majoriteten av respondenterna tillhör åldersgruppen 25–34 år (se Figur 5). Detta innebär sannolikt en viss överrepresentation av digitalt vana och aktiva lantbrukare, vilket kan påverka resultatet kring cybersäkerhetsbeteenden. En bidragande faktor till detta kan vara att enkäten primärt distribuerades via sociala medier.

4.1.2 Digitala system och uppkoppling



Figur 6. Förekomst av digitala system på gårdarna.

Resultatet visar att användningen av digitala system hos de svarande är omfattande, framför allt ekonomiprogram, GPS/autostyrning och växtodlingsprogram (se Figur 6). Även sensorer och uppkopplade maskiner förekommer i stor utsträckning. GPS-styrning används för att förbättra precisionen vid fältarbete, medan växtodlingsprogram och ekonomiprogram stödjer planering, dokumentation och administration. Sensorerna kan användas till övervakning av väder, temperatur, markfuktighet, lagerstatus och stallmiljö. Inom animalieproduktion kan det handla om övervakning av utfodring och ventilation. Det innebär att flera centrala funktioner i verksamheten är beroende av den digitala tekniken och fungerande kommunikation mellan dessa system.



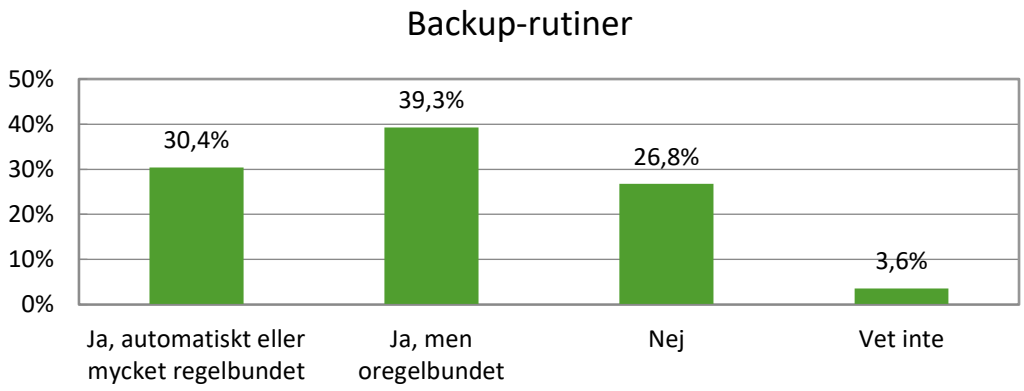
Figur 7. Frekvens av tekniska störningar i verksamheten.

En betydande andel (66 %) uppger att fjärrstyrning av system förekommer, antingen genom leverantör eller genom egen åtkomst (resultatet visas ej i figur, se fråga i bilaga 1). Ungefär hälften (51 %) har svarat att de själva primärt ansvarar för IT och digitala systemen. Tekniska störningar är relativ vanligt förekommande, där cirka 30 % upplever problem med internet eller teknik minst en gång i månaden och hela 58 % någon gång per år (se Figur 7).

Sammantaget visar resultatet att digitalisering är en central del av lantbruket, samtidigt som systemen är beroende av fungerande uppkoppling och ofta hanteras utan extern IT-kompetens.

4.1.3 Skyddsåtgärder i praktiken

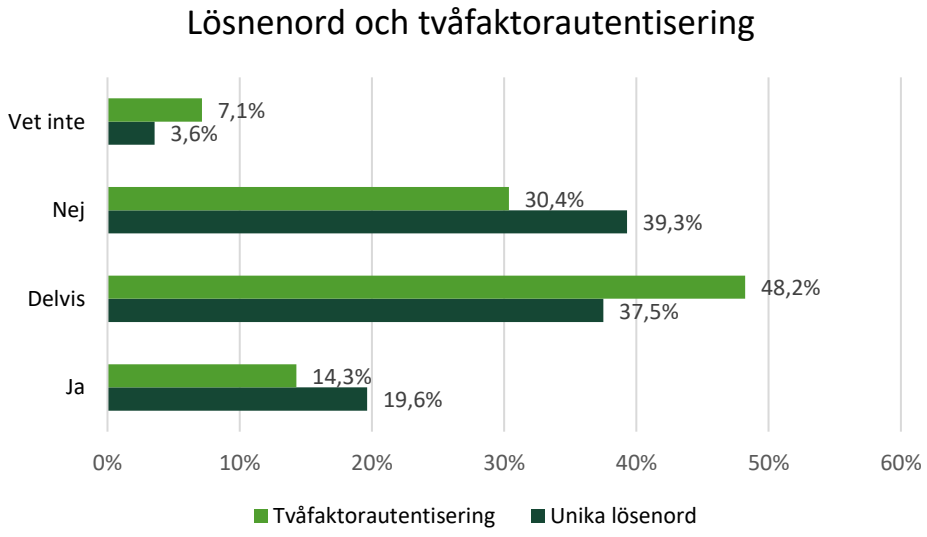
Resultaten visar tydliga brister i grundläggande cybersäkerhetsrutiner. Endast 30 % uppgav att de genomför regelbunden säkerhetskopiering av viktiga filer och data, medan en stor andel antingen saknade backuprutiner helt, eller endast genomförde detta oregelbundet (se Figur 8). Användningen av grundläggande kontoskydd var också begränsad. Nästan 40 % uppgav att de inte använde unika lösenord för viktiga konton och endast 14 % använde 2FA (tvåfaktorautentisering) i större utsträckning (se Figur 9).



Figur 8. Förekomst av säkerhetskopiering av data.

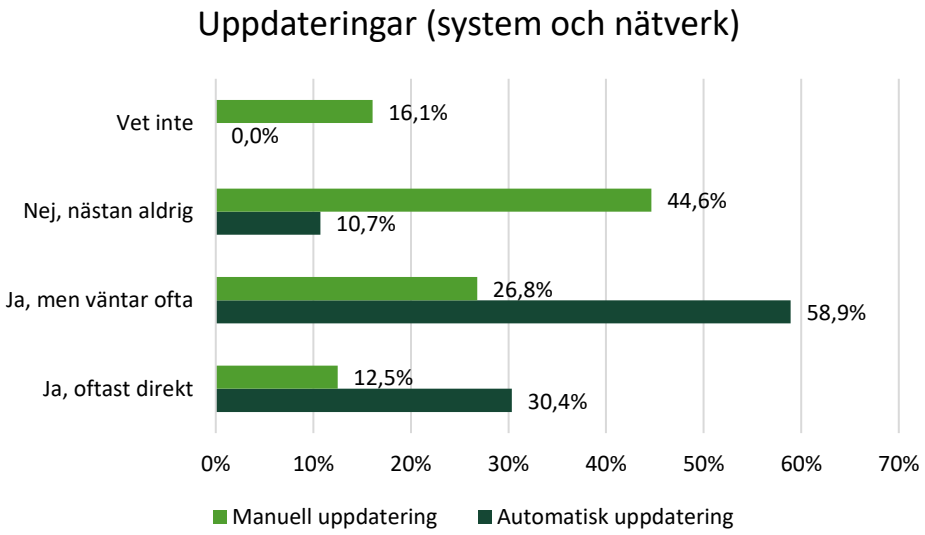
Även uppdateringsrutiner visade tydliga brister. Många respondenter uppgav att de ofta väntar med att installera uppdateringar eller att de nästan aldrig genomför manuella uppdateringar av system (se Figur 10). Endast en mindre andel uppgav att de installerar uppdateringar direkt när de blir tillgängliga.

Separata nätverk för gäster var också ovanligt förekommande. Endast 14 % uppgav att de hade någon form av nätverksseparering på gården (visas ej i figur).



Figur 9. Användning av lösenord och tvåfaktorautentisering.

Vidare saknade 77 % en plan för hur IT-relaterade incidenter ska hanteras (visas ej i figur). Detta innebär att många av lantbrukarna saknar rutiner för hur driften ska upprätthållas vid exempelvis systemfel, dataintrång eller driftstörningar.

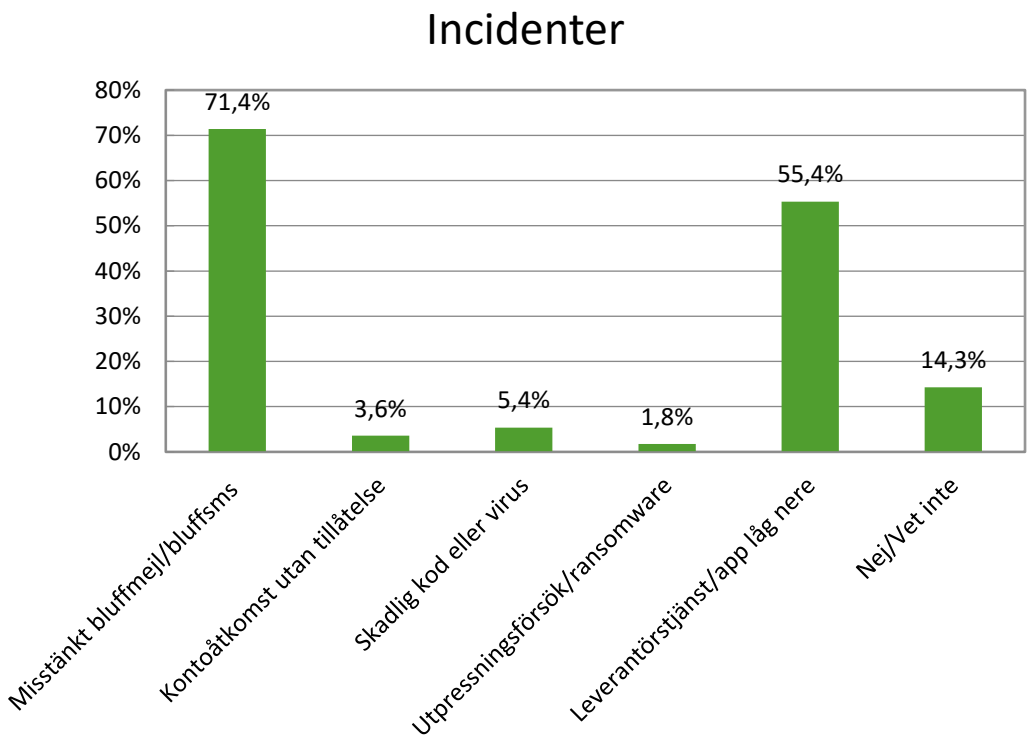


Figur 10. Rutiner för system- och säkerhetsuppdateringar.

Resultaten visar därmed att centrala skyddsåtgärder ofta saknas eller används i begränsad utsträckning. Detta tyder på att den praktiska cybersäkerhetsnivån i många fall är låg.

4.1.4 Incidenter och erfarenheter

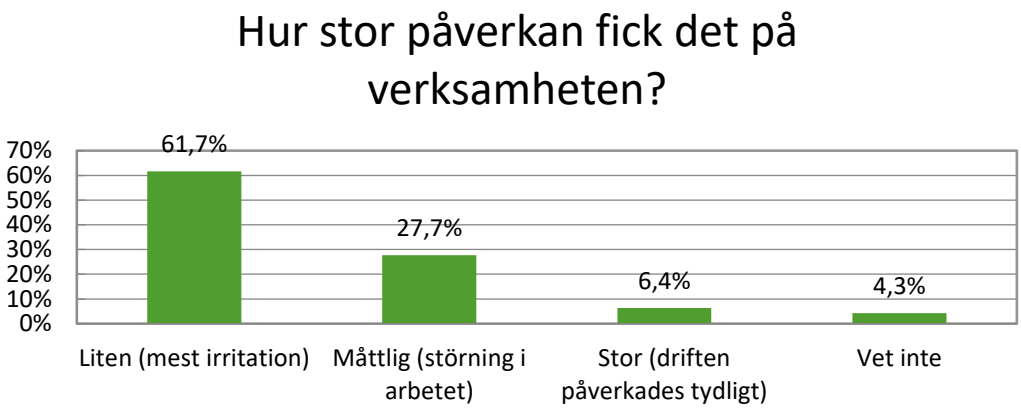
Den vanligaste typen av incident är misstänkta bluff-mejl eller bluff-sms (phishing), vilket 71 % av respondenterna uppger att de upplevt under de senaste två åren (se Figur 11). Även driftstörningar i leverantörssystem är vanligt förekommande och rapporterades av 55 % av respondenterna. Övriga incidenter, såsom virus, obehörig åtkomst eller ransomware förekommer i betydligt mindre omfattning.



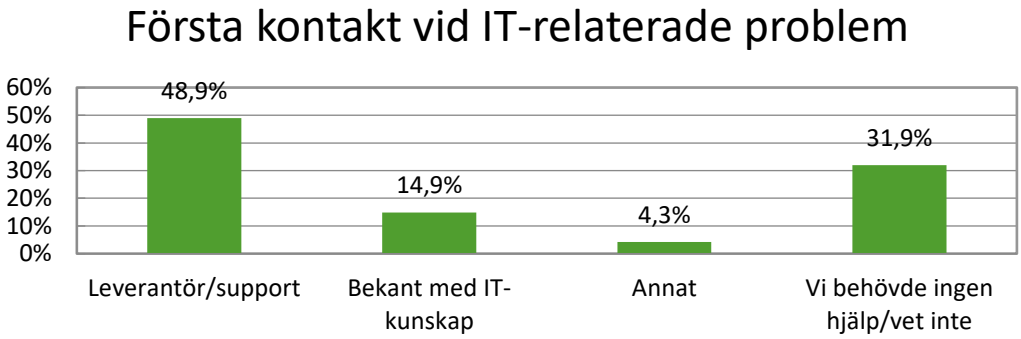
Figur 11. Förekomst av cybersäkerhetsrelaterade incidenter.

De flesta incidenter har haft begränsad påverkan och beskrivs främst som mindre störningar. Samtidigt uppger en mindre andel (6 %) att incidenter har haft en tydlig påverkan på driften (se Figur 12).

Vid behov av hjälp vänder sig respondenter främst till leverantörer eller extern support (se Figur 13), vilket visar på ett beroende av externa aktörer vid hantering av problem. Resultaten visar att cyberrelaterade händelser är relativ vanliga, även om konsekvenserna i de flesta fall är begränsade.



Figur 12. Upplevd påverkan av cyberincidenter på verksamheten.

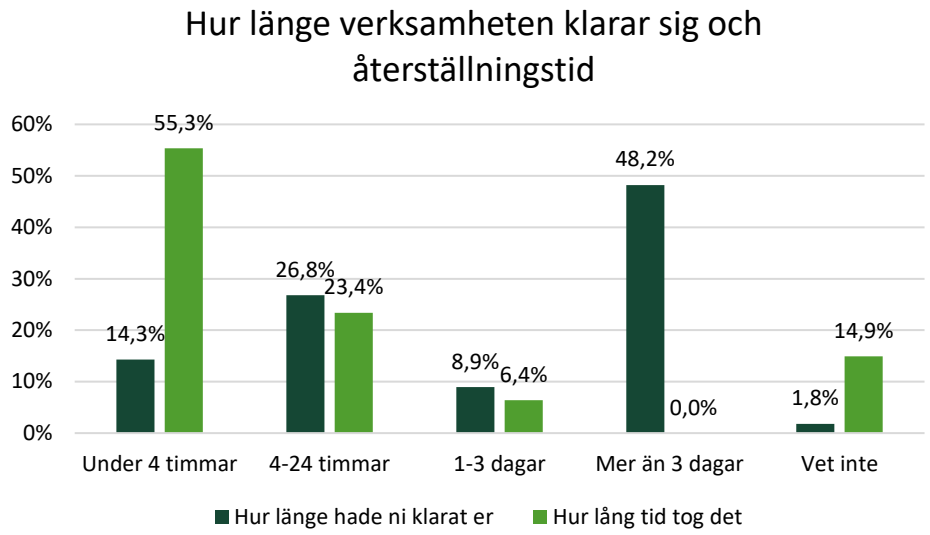


Figur 13. Första kontakt vid IT-relaterade problem.

Figur 14 visar att många respondenter bedömer att verksamheten kan fortsätta under en begränsad period även om viktiga system slås ut. Samtidigt varierar uthålligheten mellan olika produktionsgrenar. Tabell 2 visar skillnaden mellan produktionsgrenarna gällande uppskattad uthållighet och återställningstid.

Mjölk- och fjäderfäproduktionen visade på den lägsta uthålligheten vid systemstopp, där verksamheten endast bedömdes kunna fungera under några timmar utan viktiga system. Växtodling och nötköttsproduktion hade en generellt längre uthållighet.

Trots detta var återställningstiden i de flesta fall relativt kort. En majoritet uppgav att normal drift kunde återupptas inom fyra timmar.



Figur 14. Uppskattad drifttålighet vid IT-relaterade störningar.

Tabell 2. Jämförelse av genomsnittlig uthållighet och återställningstid mellan de olika produktionsgrenarna. Enheten för Uthållighet och Återställningstid är ett snitt av svarsalternativ, där det finns 4 svarsalternativ.

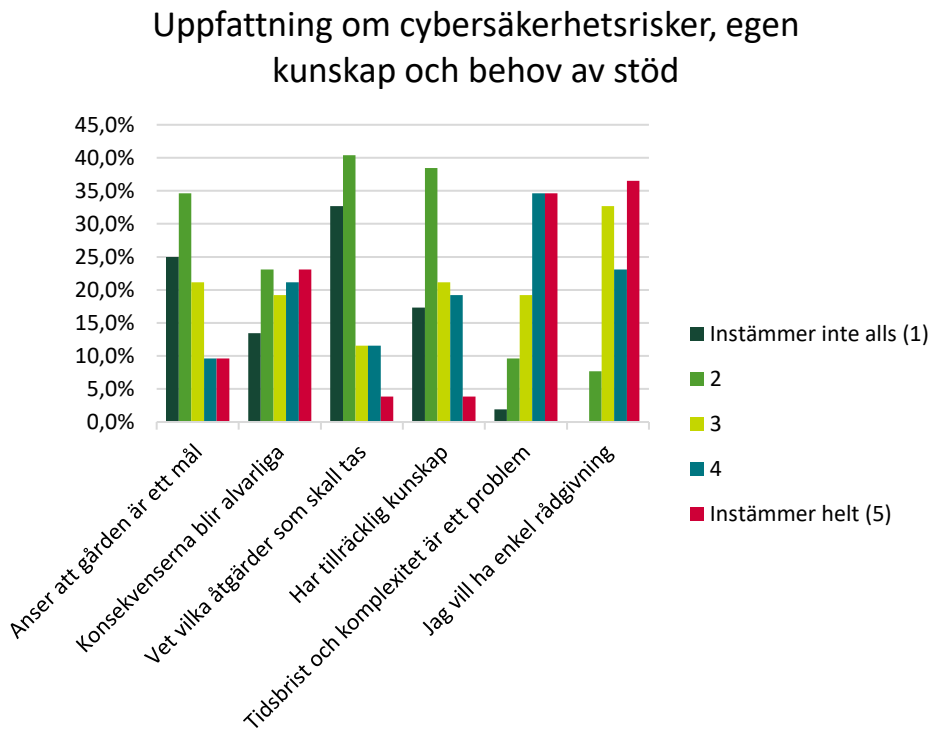
Produktion	Uthållighet	Motsvarar tid	Återställningstid	Motsvarar tid
Växtodling	3,1	1-3 dagar	1,6	4-24 timmar
Mjölk	2,1	4-24 timmar	1,0	Under 4 timmar
Nötkött	3,5	Mer än 3 dagar	1,1	Under 4 timmar
Gris	2,1	4-24 timmar	1,5	4-24 timmar
Fjäderfä	1,3	Under 4 timmar	1,5	4-24 timmar
Får/get	4,0	Mer än 3 dagar	2,0	4-24 timmar
Blandat Lantbruk	2,7	1-3 dagar	1,3	Under 4 timmar

4.1.5 Upplevd sårbarhet och cybersäkerhet

Resultatet visar en relativ låg riskuppfattning. Endast en mindre andel upplever att deras gård är ett sannolikt mål för cyberangrepp, samtidigt som många anser att konsekvenserna skulle kunna bli allvarliga (se Figur 15). Detta tyder på en diskrepans mellan upplevd risk och konsekvens.

Många respondenter uppgav även att de saknar tillräcklig kunskap för att genomföra grundläggande säkerhetsåtgärder och att tidsbrist och komplexitet gör att cybersäkerheten prioriteras ned.

Resultatet visar därmed att cybersäkerhet ofta uppfattas som viktigt, men att det samtidigt är svårt att prioritera i det dagliga arbetet.

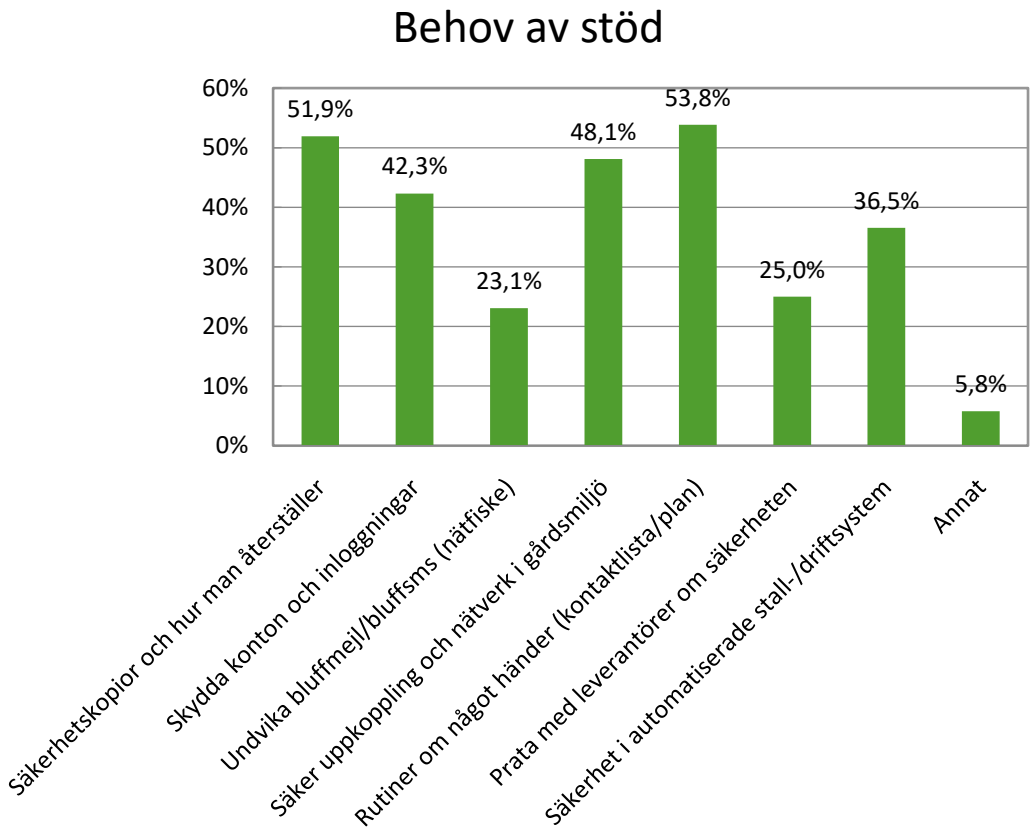


Figur 15. Uppfattning om cybersäkerhet och egen kunskap.

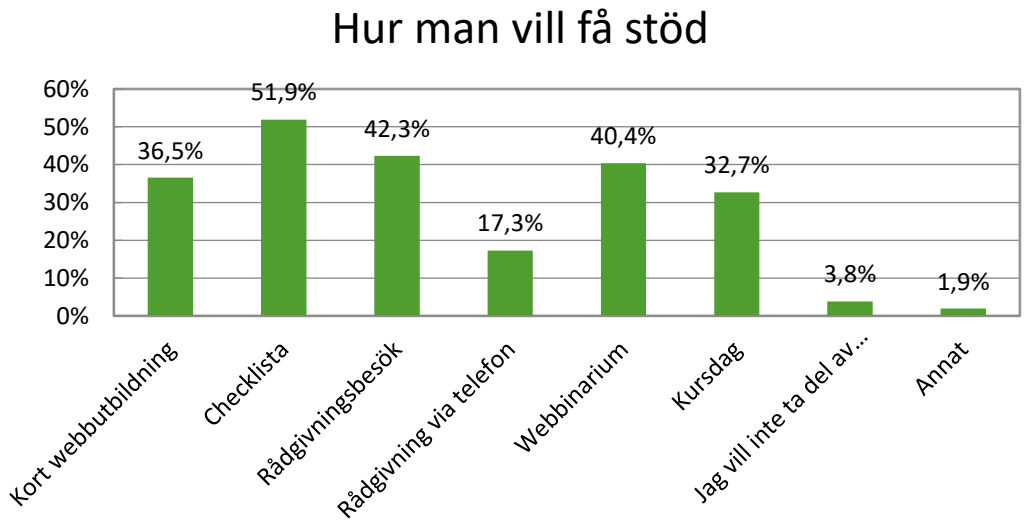
4.1.6 Behov av stöd

Det fanns ett tydligt behov av stöd inom flera områden kopplade till cybersäkerhet. De mest efterfrågade områdena är rutiner vid incidenter, säkerhetskopiering och nätverkssäkerhet (se Figur 16).

Även stöd kring skydd av konton och inloggningar samt säkerhet i automatiserade system efterfrågades. När det gäller former för stöd var checklistor den mest efterfrågade lösningen, följt av rådgivning, webbinarier och kortare webbutbildningar (se Figur 17). Endast en liten andel uppgav att de inte var intresserade av något stöd. Resultatet visar att lantbrukare främst efterfrågar praktiska och enkla lösningar.



Figur 16. Efterfrågade områden för stöd inom cybersäkerhet.



Figur 17. Föredragna former för rådgivning och utbildning.

5. Analys och diskussion

I analysen tolkas resultatet utifrån studiens sociotekniska perspektiv och de tre dimensionerna: teknisk, organisatorisk/mänsklig samt extern och institutionell dimension.

Resultaten visar tydligt att lantbruket har genomgått en omfattande digitalisering, där majoriteten av respondenterna använder flera uppkopplade system i sin dagliga verksamhet. Samtidigt framkommer betydande brister i grundläggande cybersäkerhetsrutiner, såsom säkerhetskopiering och kontoskydd i form av lösenordshantering och tvåfaktorautentisering.

Detta visar på en obalans mellan graden av digitalisering och nivån på cybersäkerheten. Ur ett sociotekniskt perspektiv innebär detta att den tekniska utvecklingen inte har följts av en liknande utveckling i användarbeteende och rutiner på de olika gårdarna/verksamheterna. På grund av det blir cybersäkerhet inte bara en teknisk fråga, utan ett resultat av samspelet mellan teknik, människa och organisationen.

En observation från resultatet är att riskuppfattningen generellt är låg, trots att en stor del av respondenterna har erfarenhet av incidenter, såsom nätfiske (phishing) och driftstörningar. Detta tyder på att exponering för risk inte nödvändigtvis leder till ökad medvetenhet. Tidigare forskning visar också att utbildningen och medvetenheten kring cybersäkerhet i lantbruket och dess leveranskedjor är otillräcklig (Adewusi et al. 2022).

Resultatet ser ut som det gör på grund av en låg riskuppfattning, där cyberhot upplevs som avlägsna och fokuset istället ligger på fysiska risker i verksamheten. Tidigare forskning visar att de flesta lantbrukare inte ser nätverksproblem som ett betydande hot och att medvetenheten om cybersäkerhet ofta är låg, trots att IT ansågs som kritisk för verksamheten (Nikander et al. 2020).

Resursbegränsningar kan också vara en bidragande faktor, då mindre och medelstora företag har begränsat med tid och kompetens inom ämnet. Komplexiteten i tekniken kan göra att lösningar kopplade till cybersäkerhet kan upplevas som svåra att implementera. Det finns också en avsaknad av riktat stöd i nuläget, där det idag saknas anpassade utbildningar för lantbrukare.

Studien visar att åtgärder bör fokusera på enkla säkerhetsrutiner såsom backup, lösenordshantering och tvåfaktorautentisering. Praktiska checklistor och rådgivning anpassad till lantbruket efterfrågades också. Detta tyder på att förbättrad

cybersäkerhet inte kräver avancerad teknik, utan istället en bättre implementering av grundläggande åtgärder.

5.1 Teknisk dimension

Resultaten visar att digitala system är brett implementerade, framför allt inom ekonomi, och växtodlingsprogram och GPS-styrning. Även sensorer, uppkopplade maskiner och automatiserade system förekommer i stor utsträckning.

Samtidigt uppvisar många verksamheter tydliga brister i grundläggande tekniska skyddsåtgärder. Ur CIA-triadens perspektiv innebär detta flera typer av sårbarheter. Bristande säkerhetskopiering hotar tillgängligheten genom att viktiga system och data riskerar att bli otillgängliga vid incidenter. Svaga lösenord och begränsad användning av 2FA (tvåfaktorautentisering) påverkar konfidentialitet genom att obehöriga lättare kan få åtkomst till system och konton. Uteblivna uppdateringar kan samtidigt hota integriteten genom att sårbarheter i system inte åtgärdas. Detta ligger i linje med tidigare forskning som visar att IoT-baserade system i lantbruket ökar attackytan och därmed sårbarheten (Kristen et al. 2021; Alahe et al. 2024).

Trots att många respondenter rapporterat någon form av incident har konsekvenserna i de flesta fall varit begränsade. Detta kan skapa en falsk känsla av säkerhet, där avsaknaden på allvarliga konsekvenser minskar incitamentet att investera i cybersäkerhet.

Samtidigt visar resultaten att vissa produktionsgrenar, särskilt mjölk- och fjäderfäproduktion, är mycket beroende av fungerande system och att de inte klarar sig utan systemen länge perioder. Detta innebär att konsekvenserna av framtida cyberrelaterade incidenter potentiellt kan bli allvarliga.

5.2 Organisatorisk och mänsklig dimension

Cybersäkerheten hanteras i stor utsträckning av lantbrukaren själv, ofta utan någon formell utbildning eller tydliga rutiner. Samtidigt upplever många att de saknar tillräcklig kunskap och att tidsbrist gör att säkerhetsfrågor prioriteras ned. Detta går att koppla till det sociotekniska perspektivet, där mänskliga faktorer spelar en avgörande roll för säkerhetsnivån. Säkerhetsnivån avgörs inte enbart av vilka tekniska lösningar som finns tillgängliga, utan också av användarnas kunskap, prioriteringar och beteenden. Enkla säkerhetsåtgärder kan få stor betydelse om de används konsekvent, medan avancerade system ger begränsat skydd om användaren saknar kunskap eller rutiner.

Den låga användningen av tvåfaktorautentisering kan förklaras av en upplevd komplexitet, brist på kunskap och en låg upplevd risk. Detta överensstämmer med tidigare forskning som identifierat bristande säkerhetsmedvetenhet som en central sårbarhet i lantbruket (Adewusi et al. 2022).

5.3 Extern och institutionell dimension

Studien visar att många lantbrukare är beroende av externa aktörer vid tekniska problem och cyberrelaterade incidenter. Leverantörer är ofta den första kontakten vid problem. Detta innebär att cybersäkerheten delvis ligger utanför lantbrukarens egen kontroll. Om leverantörer drabbas av driftstörningar eller säkerhetsproblem kan det få konsekvenser även för gårdens verksamhet.

Samtidigt finns det en efterfrågan på stöd och rådgivning, där respondenterna främst vill ha checklistor, rådgivning och enkla utbildningar. Detta indikerar att nuvarande stöd kring cybersäkerhet inte är tillräckligt anpassat till lantbrukets praktiska förutsättningar. Många verksamheter saknar sannolikt både tid och resurser för mer omfattande utbildningsinsatser.

Tidigare forskning visar att komplexa leveranskedjor och beroende till tredjepartsaktörer utgör en central risk inom digitaliserat jordbruk (Adewusi et al. 2022; Olateju 2025), vilket bekräftas av resultaten i denna studie.

5.4 Framtida åtgärder och forskning

Det finns flera möjligheter att stärka cybersäkerheten i lantbruket. Eftersom många lantbrukare efterfrågar praktiskt stöd kan enkla verktyg och rådgivning vara ett bra sätt att öka säkerhetsnivån. Många av de brister som identifierats i studien handlar om grundläggande rutiner och hur IT-relaterade problem ska hanteras.

I takt med att digitaliseringen ökar så ökar också beroendet av leverantörer och externa tjänster. Därför behöver cybersäkerheten ses som ett gemensamt ansvar mellan lantbrukare, leverantörer, rådgivningsorganisationer och myndigheter. Ett ökat samarbete mellan dessa aktörer skulle kunna bidra till att minska den digitala sårbarheten inom sektorn.

Samtidigt finns behov av fortsatt forskning inom området. Denna studie bygger på lantbrukarnas egna uppfattningar och erfarenheter, men framtida studier skulle även kunna inkludera tekniska analyser av gårdars faktiska säkerhetsnivå. Det finns

också behov av mer forskning kring hur olika produktionsgrenar påverkas av cyberincidenter, vilka skyddsåtgärder som ger störst effekt i praktiken samt mer noggrant hur rådgivningen och utbildningen kan utformas för att nå olika grupper av lantbrukare.

5.5 Metoddiskussion

En styrka med studien är att enkätmetoden möjliggör insamling av data från ett relativt stort antal respondenter på kort tid. Detta ger en bred överblick av lantbrukares uppfattningar och erfarenheter av cybersäkerhet.

Samtidigt finns begränsningar eftersom urvalet baseras på sociala medier. Det kan göra att resultatet inte är fullt representativt för alla lantbrukare. Det finns även en risk att respondenterna har olika nivåer av kunskap om digital teknik, vilket kan påverka hur frågorna tolkas.

Studiens validitet bedöms som god då frågorna är utformade för att passa studiens syfte. Däremot kan tillförlitligheten påverkas av att svaren bygger på deltagarnas egna uppfattningar och kunskap. Det finns exempelvis en risk att säkerhetsrutiner överskattas eller att tidigare incidenter glöms bort eller inte rapporteras. Skillnader i teknisk kunskap kan också påverka hur vissa frågor tolkas.

Resultaten bör tolkas med försiktighet då urvalet baseras på sociala medier och därmed sannolikt överrepresenterar yngre och mer digitalt aktiva lantbrukare. Detta kan innebära att den faktiska cybersäkerhetsnivån i populationen är ännu lägre än vad resultatet visar.

6. Slutsatser

Resultaten i denna studie ligger i stor utsträckning i linje med tidigare forskning kring cybersäkerhet i lantbruket. Flera tidigare studier beskriver hur digitalisering och uppkopplade system ökar sårbarheten för cyberrelaterade incidenter samt hur begränsad kunskap och lågt säkerhetsmedvetande utgör risker.

Det som denna studie kan bidra med är en konkret bild av hur detta ser ut på gårdsnivå i Sverige. Resultaten visar att problemen inte enbart är teoretiska, utan också praktiska och relativt utbredda. Samtidigt visar studien att många av de mest centrala säkerhetsbristerna handlar om grundläggande rutiner snarare än tekniska problem.

Studien visar att lantbruket i hög grad har digitaliserats och att användningen av uppkopplade system är omfattande. Samtidigt finns betydande brister i grundläggande cybersäkerhetsrutiner, vilket innebär att många verksamheter är sårbara för cyberrelaterade incidenter och risker för konfidentialitet, riktighet och tillgänglighet.

Lantbrukare upplever generellt en låg risk till att själva bli utsatta för cyberangrepp, trots att de ofta har erfarenhet av till exempel nätfiske (phishing) och driftstörningar. Det visar att det finns en diskrepans mellan faktisk exponering och upplevd risk.

En central slutsats är att cybersäkert inom lantbruket inte enbart är en teknisk fråga, utan det påverkas även till stor del av kunskap, och beteende samt organisatoriska förutsättningar. Den sociotekniska analysen visar att brister i kompetens, rutiner och prioritering är faktorer som kan påverka säkerhetsnivån.

För att minska den digitala sårbarheten behöver cybersäkerhet bli en mer integrerad del av det dagliga arbetet i lantbruket. Många av de mest centrala säkerhetsbristerna kan sannolikt minska genom relativt enkla och kostnadseffektiva åtgärder. Studien visar även att det finns ett tydligt behov av stöd i form av rådgivning, utbildning och praktiska verktyg.

Framtida arbete inom ämnet bör fokusera på att öka medvetenheten om cybersäkerhetsriskerna, samt att ta fram konkreta och användarvänliga lösningar som kan integreras i det dagliga arbetet.

Referenser

Adewusi, A.O., Chiekezie, N.R. & Eyo-Udo, N.L. (2022). Cybersecurity threats in agriculture supply chains: A comprehensive review. *World Journal of Advanced Research and Reviews*, 15 (3), 490–500. https://doi.org/10.30574/wjarr.2022.15.3.0888

Alahe, M.A., Wei, L., Chang, Y., Gummi, S.R., Kemeshi, J., Yang, X., Won, K. & Sher, M. (2024). Cyber security in smart agriculture: Threat types, current status, and future trends. *Computers and Electronics in Agriculture*, 226, 109401. https://doi.org/10.1016/j.compag.2024.109401

Angyalos, Z., Botos, S. & Szilágyi, R. (2021). The importance of cybersecurity in modern agriculture. *AGRÁRINFORMATIKA / JOURNAL OF AGRICULTURAL INFORMATICS*, 12 (2), 1–8

Anthropic (2026). *System Card: Claude Mythos Preview*. https://www-cdn.anthropic.com/08ab9158070959f88f296514c21b7facce6f52bc.pdf [2026-04-14]

BBC (2021). *Meat giant JBS pays $11m in ransom to resolve cyber-attack*. https://www.bbc.com/news/business-57423008 [2026-06-09]

Berchtold, J. (2024). *Ransomware attack on farmer - cow dies*. *ReedSmith*. https://www.reedsmith.com/our-insights/blogs/viewpoints/102jglp/ransomware-attack-on-farmer-cow-dies/ [2026-06-09]

Campoverde-Molina, M. & Luján-Mora, S. (2025). Cybersecurity in smart agriculture: A systematic literature review. *Computers & Security*, 150, 104284. https://doi.org/10.1016/j.cose.2024.104284

Carlini, N., Cheng, N., Keane, L., Moore, M., Nasr, M., Prabhushankar, V., Xiao, W., Angulu, H., Asher, E.B., Bow, J., Bradwell, K., Buchanan, B., Forsythe, D., Freeman, D., Gaynor, A., Ge, X., Graham, L., Guru, K., Lakhani, H., McNiece, M., Mehrara, M., Nichol, R., Pirzada, A., Porter, S., Terzis, A. & Troy, K. (2026). *Assessing Claude Mythos Preview's cybersecurity capabilities*. *red.anthropic.com*. https://red.anthropic.com/2026/mythos-preview/ [2026-04-14]

CIA-Triad (2024). *CIA-triaden - Vad är CIA triaden för informationssäkerhet*. https://ciatriad.se/vad-ar-cia-triad/ [2026-04-13]

Goldenits, G. & Neubauer, T. (2025). Taxonomy of cybersecurity considerations in agriculture. *Computers and Electronics in Agriculture*, 237, 110724. https://doi.org/10.1016/j.compag.2025.110724

Gupta, M., Abdelsalam, M., Khorsandroo, S. & Mittal, S. (2020). Security and Privacy in Smart Farming: Challenges and Opportunities. *IEEE Access*, 8, 34564–34584. https://doi.org/10.1109/ACCESS.2020.2975142

Kristen, E., Kloibhofer, R., Díaz, V.H. & Castillejo, P. (2021). Security Assessment of Agriculture IoT (AIoT) Applications. *Applied sciences*, 11 (13), 5841-. https://doi.org/10.3390/app11135841

Lantmännen (2022). *Lantmännen säkrar omhändertagandet av skörden trots IT-störningar*. *Lantmännen.se*. https://www.lantmannen.se/om-lantmannen/press-och-nyheter/pressmeddelanden/2022/lantmannen-sakrar-omhandertagandet-av-skorden-trots-it-storningar/ [2026-04-10]

Lundström, C. & Lindblom, J. (2018). Considering farmers' situated knowledge of using agricultural decision support systems (AgriDSS) to Foster farming practices: The case of CropSAT. *Agricultural Systems*, 159, 9–20. https://doi.org/10.1016/j.agsy.2017.10.004

Maraveas, C., Rajarajan, M., Arvanitis, K.G. & Vatsanidou, A. (2024). Cybersecurity threats and mitigation measures in agriculture 4.0 and 5.0.

Smart Agricultural Technology, 9, 100616. https://doi.org/10.1016/j.atech.2024.100616
MSB (u.å.). *Klassningsmodell*. *Metodstödet för systematiskt informationssäkerhetsarbete*. https://metodstod-informationssakerhet.msb.se/sv/utforma/klassningsmodell/ [2026-05-07]
Neethirajan, S. (2025). Safeguarding digital livestock farming - a comprehensive cybersecurity roadmap for dairy and poultry industries. *Frontiers in Big Data*, 8, 1556157. https://doi.org/10.3389/fdata.2025.1556157
Nikander, J., Manninen, O. & Laajalahti, M. (2020). Requirements for cybersecurity in agricultural communication networks. *Computers and Electronics in Agriculture*, 179, 105776. https://doi.org/10.1016/j.compag.2020.105776
Olateju, O.O. (2025). Blockchain and Cybersecurity Integration for Secure and Resilient Agricultural Supply Chains in the United States. *Asian Journal of Advances in Agricultural Research*, 25 (4), 126–138. https://doi.org/10.9734/ajaar/2025/v25i4606
Rijswijk, K., Klerkx, L., Bacco, M., Bartolini, F., Bulten, E., Debruyne, L., Dessein, J., Scotti, I. & Brunori, G. (2021). Digital transformation of agriculture and rural areas: A socio-cyber-physical system framework to support responsibilisation. *Journal of Rural Studies*, 85, 79–90. https://doi.org/10.1016/j.jrurstud.2021.05.003
Saiz-Rubio, V. & Rovira-Más, F. (2020). From Smart Farming towards Agriculture 5.0: A Review on Crop Data Management. *Agronomy*, 10 (2), 207. https://doi.org/10.3390/agronomy10020207
Tunberg, M., Engström, J., Rydberg, A., Gilbertsson, M., Larsen, C.P. & Torfgård, L. (2022). Förstudie: Förslag till nationellt kunskapsnav för digitaliserat jordbruk.
Warkentin, M. & Orgeron, C. (2020). Using the security triad to assess blockchain technology in public sector applications. *International Journal of Information Management*, 52, 102090. https://doi.org/10.1016/j.ijinfomgt.2020.102090

Bilaga 1

Frågor till enkät

Gårdsprofil

Vilken typ av produktion passar bäst in på din gård?

- Växtodling
- Mjölk
- Nötkött
- Gris
- Fjäderfä
- Får/get
- Blandat Lantbruk
- Annat

Ungefär hur stor är verksamheten?

- 1 person arbetar regelbundet på gården
- 2-3 personer
- 4-10 personer
- Fler än 10 personer

Hur "digital" upplever du att gården är?

- Nästan inget digitalt
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- Mycket digitalt/uppkopplat

Vilken åldersgrupp tillhör du?

- Under 18 år
- 18-24 år
- 25-34 år
- 35-44 år
- 45-54 år
- 55-64 år

- 65 år eller äldre
- Vill ej ange

Digitala system och uppkoppling

Vilka system används på gården?

- GPS/autostyrning i maskiner
- Maskiner som skickar data (fjärrövervakning av maskiner)
- Program/app för växtodlingsplanering eller journaler
- Ekonomiprogram/bokföring i dator eller molntjänst
- Sensorer (t.ex. väder, lager, temperatur, stallmiljö)
- Kamera/övervakning kopplad till internet
- Automatisering i djurstall (t.ex. mjölkrobot, utfodring, ventilation/klimat)
- Jag använder nästan inget av detta

Hur ofta har du problem med internet/uppkoppling som stör arbetet?

- Aldrig
- Någon gång per år
- Någon gång per månad
- Varje vecka eller oftare
- Vet inte

Hur ofta har du problem med andra tekniska störningar?

- Aldrig
- Någon gång per år
- Någon gång per månad
- Varje vecka eller oftare
- Vet inte

Har någon leverantör (eller du själv) möjlighet att fjärrstyra något system på gården?

- Ja
- Nej
- Vet inte

Vem ansvarar primärt för IT/digitala system?

- Jag själv
- Anställd
- Extern IT-leverantör (extern firma som sköter IT, support eller drift)
- Utrustningsleverantör (leverantör av maskin/utrustning som även sköter systemet)
- Blandat

Skyddsåtgärder i praktiken

Har du en rutin för att spara kopior på viktiga filer eller data?

- Ja, automatiskt eller myket regelbundet
- Ja, men oregelbundet
- Nej
- Vet inte

Använder du unika lösenord för viktiga konton?

- Ja
- Delvis
- Nej
- Vet inte

Används tvåfaktorautentisering (inloggning med två steg, t.ex. med hjälp av mobil eller sms) på viktiga k

- Ja, på de flesta viktiga konton
- Ja, på något konto
- Nej
- Vet inte

Uppdaterar du dator/mobil och appar när de frågar om uppdatering?

- Ja, oftast direkt
- Ja, men jag väntar ofta
- Nej, nästan aldrig
- Vet inte

Uppdaterar du system och brandvägg manuellt?

- Ja, oftast direkt
- Ja, men väntar ofta
- Nej, nästan aldrig
- Vet inte

Har du ett separat nätverk för gäster/besökare gentemot gårdens egna system?

- Ja
- Nej
- Vet inte

Finns det någon enkel plan för vad ni gör om ett viktigt system slutar fungera på grund av IT-problem?

- Ja
- Nej
- Vet inte

Hur länge hade ni klarat er om ett viktigt system slutar fungera?

- Under 4 timmar
- 4-24 timmar
- 1-3 dagar
- Mer än 3 dagar
- Vet inte

Incidenter och erfarenheter

Har du under de senaste 24 månaderna upplevt någon av följande händelser?

- Misstänkt bluffmejl/bluffsms (någon vill att du ska klicka på länk eller logga in)
- Någon har kommit åt ett konto utan tillåtelse
- Skadlig kod eller virus
- Utpressningsförsök/ransomware (system låses och man krävde betalning)
- Leverantörstjänst/app låg nere och störde arbetet
- Vet inte

Hur stor påverkan fick det på verksamheten?

- Liten (mest irritation)
- Måttlig (störning i arbetet)
- Stor (driften påverkades tydligt)
- Vet inte

Hur långt tid tog det innan ni var i normal drift igen?

- Under 4 timmar
- 4-24 timmar
- 1-3 dagar
- Mer än 3 dagar
- Vet inte

Om ni behövde hjälp, vart vände ni er i första hand?

- Leverantör/support
- Bekant med IT-kunskap
- Annat
- Vi behövde ingen hjälp/vet inte

Hur ser du på risker och stöd? 1 = instämmer inte alls
5 = instämmer helt

- Jag bedömer att min gård kan vara mål för cyberangrepp
- Om ett viktigt system slås ut skulle konsekvenserna bli allvarliga för min verksamhet
- Jag vet vilka åtgärder jag ska ta vid en cyberincident

- Jag upplever att jag har tillräcklig kunskap för att genomföra grundläggande säkerhetsåtgärder
- Tidsbrist och komplexitet gör att cybersäkerhet ofta prioriteras ned
- Jag skulle vilja ha enkel och praktisk rådgivning om digital säkerhet som passar lantbruk

Vilka områden skulle du helst vilja få hjälp med?

- o Säkerhetskopior och hur man återställer
- o Skydda konton och inloggningar
- o Undvika bluffmejl/bluffsms (nätfiske)
- o Säker uppkoppling och nätverk i gårdsmiljö (wifi/routrar/segmentering)
- o Rutiner om något händer (kontaktlista/plan)
- o Prata med leverantörer om säkerhet och fjärrsupport
- o Säkerhet i automatiserade stall-/driftsystem
- o Annat

Hur vill du ta del av stöd?

- o Kort webbutbildning
- o Checklista
- o Rådgivningsbesök
- o Rådgivning via telefon
- o Webbinarium
- o Kursdag
- o Jag vill inte ta del av stöd
- o Annat

Publicering och arkivering

Godkända självständiga arbeten (examensarbeten) vid SLU kan publiceras elektroniskt. Som student äger du upphovsrätten till ditt arbete och behöver i sådana fall godkänna publiceringen. I samband med att du godkänner publicering kommer SLU även att behandla dina personuppgifter (namn) för att göra arbetet sökbart på internet. Du kan närsomhelst återkalla ditt godkännande genom att kontakta biblioteket.

Även om du väljer att inte publicera arbetet eller återkallar ditt godkännande så kommer det arkiveras digitalt enligt arkivlagstiftningen.

Du hittar länkar till SLU:s publiceringsavtal och SLU:s behandling av personuppgifter och dina rättigheter på den här sidan:

- https://libanswers.slu.se/sv/faq/228316

☒ JA, jag, Jakob Frisk har läst och godkänner avtalet för publicering samt den personuppgiftsbehandling som sker i samband med detta

☐ NEJ, jag/vi ger inte min/vår tillåtelse till att publicera fulltexten av föreliggande arbete. Arbetet laddas dock upp för arkivering och metadata och sammanfattning blir synliga och sökbara.