MNP
DIGITAL

MNP REPORT

Cyber security on the farm

Research conducted by:

RealAgristudies
Farm Vision 2020

Wherever business takes you MNPdigital.ca

Executive summary

Cultivating resilience: Protecting Canada’s farms in a digital age

Canadian farmers are at crossroads. As agriculture embraces cutting-edge technology — things like precision farming, automation, and connected supply chains — operations are becoming more efficient and productive than ever before. Yet, these innovations bring growing vulnerabilities. Cyber threats, including ransomware, phishing, and AI-driven scams, are becoming more frequent and sophisticated. Threat actors are increasingly using artificial intelligence to create highly targeted attacks, such as deepfake emails or voice phishing, that exploit trust and human error. A single cyber incident can disrupt daily operations, cause financial losses, and erode the trust built with customers. Alarmingly, 82 percent of farmers believe they’ve never experienced a cyberattack, despite nearly half of their suppliers reporting otherwise. This disconnect highlights the urgent need for greater awareness and preparation.

Canada’s agriculture sector is a critical pillar of the national economy and food security, making it an appealing target for cybercriminals. In recent years, ransomware attacks on the food and agriculture industry have surged, as outlined in FBI alerts and global cyber intelligence reports. AI-driven scams, in particular, amplify the risks by mimicking trusted communications with alarming accuracy, making it even harder for farmers to detect and prevent attacks. Despite these threats, nearly 80 percent of Canadian farms lack a formal incident response plan, leaving them vulnerable to disruptions that could ripple through the broader food supply chain, impacting rural communities and the economy.

At MNP, we care deeply about safeguarding the future of Canadian agriculture. With over 60 years of experience working alongside farmers, we understand the unique challenges they face and the critical role they play in our society. Our approach combines practical expertise with tailored solutions to help farms protect themselves from cyber risks while continuing to innovate. By offering strategies that address both emerging threats and operational realities, we strive to empower farmers to secure their livelihoods and contribute to the resilience of Canada’s food system.

This report emphasizes an undeniable reality — cyber threats are no longer distant possibilities, they are here, evolving, and targeting the agriculture sector. AI-driven attacks are one of many risks that demand proactive solutions, but with the right tools, knowledge, and preparation, Canadian farmers can turn these challenges into opportunities for growth and resilience. Together, we can foster a secure and thriving agricultural sector that continues to nourish and sustain Canada for generations to come.

To better understand the current state of cyber security in Canada's agriculture sector, MNP partnered with RealAgristudies, a trusted leader in agriculture research. For over five years, RealAgristudies has worked closely with Canadian producers, gathering insights on the most pressing issues in the industry. By combining the expertise of RealAgriculture and Agristudies, they bring deep industry knowledge and an unparalleled ability to deliver meaningful and actionable insights.

Methodology

This study was conducted in July 2024 and involved 541 Canadian farmers, representing a broad range of farm sizes and types. Respondents, drawn from RealAgristudies' extensive insights panel, were presented with multiple-choice and attitude-based questions about their experiences and perceptions of cyber security on the farm. The findings offer a clear and statistically significant snapshot of the industry, with results accurate to within plus/minus five percent at a 95 percent confidence level.

Farmers received a personalized report that allowed them to compare their cyber security awareness and readiness against national benchmarks. This feature helped create a sense of community within the agricultural sector and encouraged farmers to assess their vulnerabilities and take proactive steps to address them.

Key learnings

The following highlights the most important observations from the report. By addressing these challenges directly, Canadian farmers can strengthen their defenses, secure their operations, and protect the future of the nation's food supply.

The disconnect in cyber security awareness

Many farmers underestimate their vulnerability to cyberattacks, with 82 percent believing they've never experienced one — despite nearly 50 percent of suppliers reporting otherwise. This gap in awareness leaves farms exposed to threats they may not even realize exist.

Preparation is lagging behind

Cyber security readiness remains low, with nearly 80 percent of farms lacking an incident response plan. Proactive planning is critical to minimize the operational and financial impact of cyber incidents.

Generational knowledge gaps

Only seven percent of farmers feel very knowledgeable about cyber security. Younger farmers tend to have greater awareness, but older generations often overestimate their safety due to limited reliance on technology. Bridging this gap is key to fostering better preparedness across all age groups.

Farms are a growing target

The increasing use of operational technologies — like GPS-guided tractors, automated feeding systems, and greenhouse controls — has made farms efficient but also more susceptible to attacks. Cybercriminals are exploiting these vulnerabilities, with phishing, malware, and ransomware identified as the top threats.

The role of partnerships and education

Collaboration with trusted partners like RealAgristudies and leveraging government resources such as Cybersecure Canada can help farmers access tools and knowledge to safeguard their operations. Awareness campaigns, tailored training, and easy-to-implement best practices can bridge critical gaps.

Cyber security experience

Cyber security experience

The digital evolution of agriculture has brought unprecedented efficiencies to farm operations but has also introduced significant vulnerabilities to cyber threats. Farmers increasingly rely on operational technology, such as automated feeding systems, livestock monitoring tools, and precision irrigation systems, to maintain productivity and profitability. However, these systems are often overlooked in cyber security planning, leaving critical infrastructure at risk.

Despite these risks, the survey revealed that 82 percent of respondents have never experienced a cyberattack — or so they believe. Our cyber security professionals suggest this figure may reflect a lack of awareness rather than reality. Many attacks, particularly phishing and ransomware, operate stealthily, compromising systems without immediate detection. This lack of preparedness is underscored by the finding that only 16 percent of respondents have an incident response plan in place. Smaller farms, in particular, face challenges due to limited resources and expertise, further increasing their exposure to cyber threats.

Social engineering tactics, such as phishing emails and business email compromises, remain the most prevalent threats to farms. Attackers exploit human error, a factor that accounts for 95 percent of cyber security incidents globally. One illustrative case involved a farmer falling victim to a fraudulent supplier website, highlighting the importance of skepticism and diligence in digital interactions.

As cyberattacks become more sophisticated and widespread, the agricultural sector must prioritize education, proactive planning, and resilience. Simple measures, like developing incident response plans and adopting basic cyber security best practices, can significantly reduce risks. The cost of inaction is steep — not only in potential financial losses but also in the disruption of vital food supply chains.

Knowledge & awareness of cyber threats

How would you rate your overall level of knowledge and awareness of cyber security and the threats they possess?

16%

I'm very knowledgeable

50%

I'm somewhat knowledgeable

36%

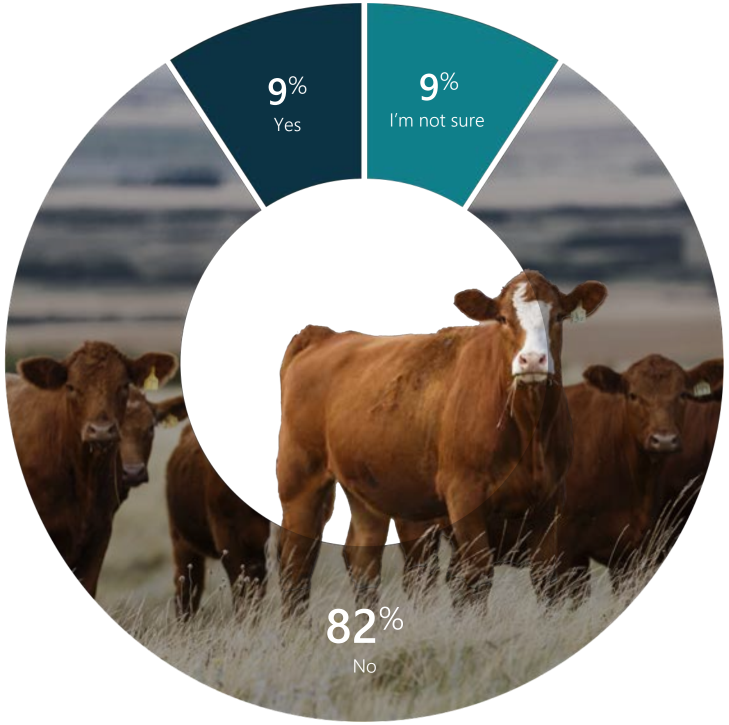
I've very little knowledge

8%

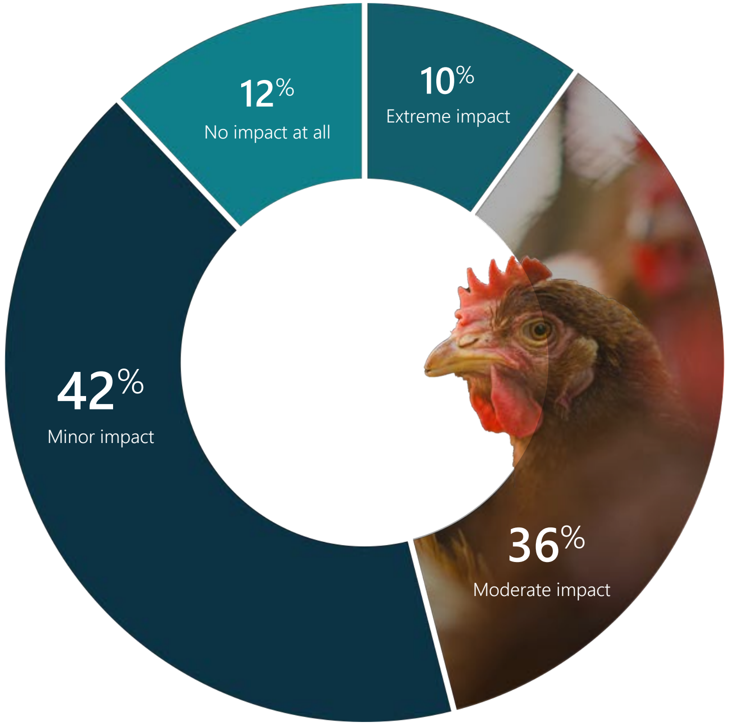
I don't really know anything

Experience with cyber attacks

Has your farm ever received a cyber attack?

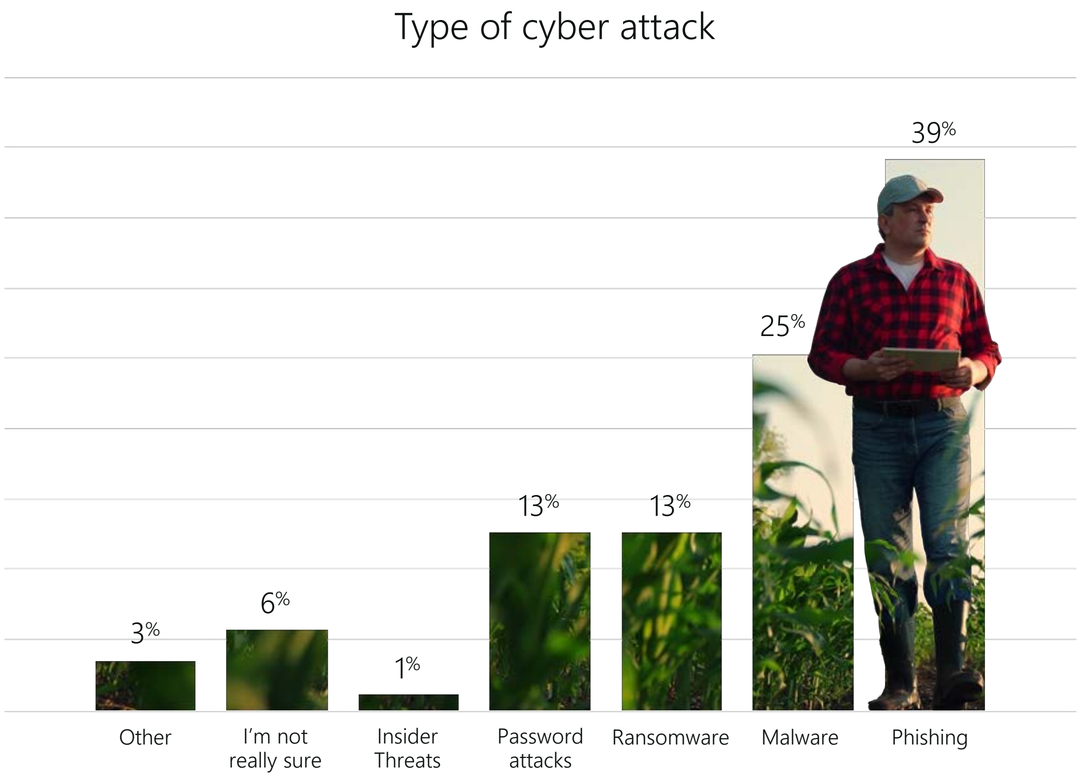


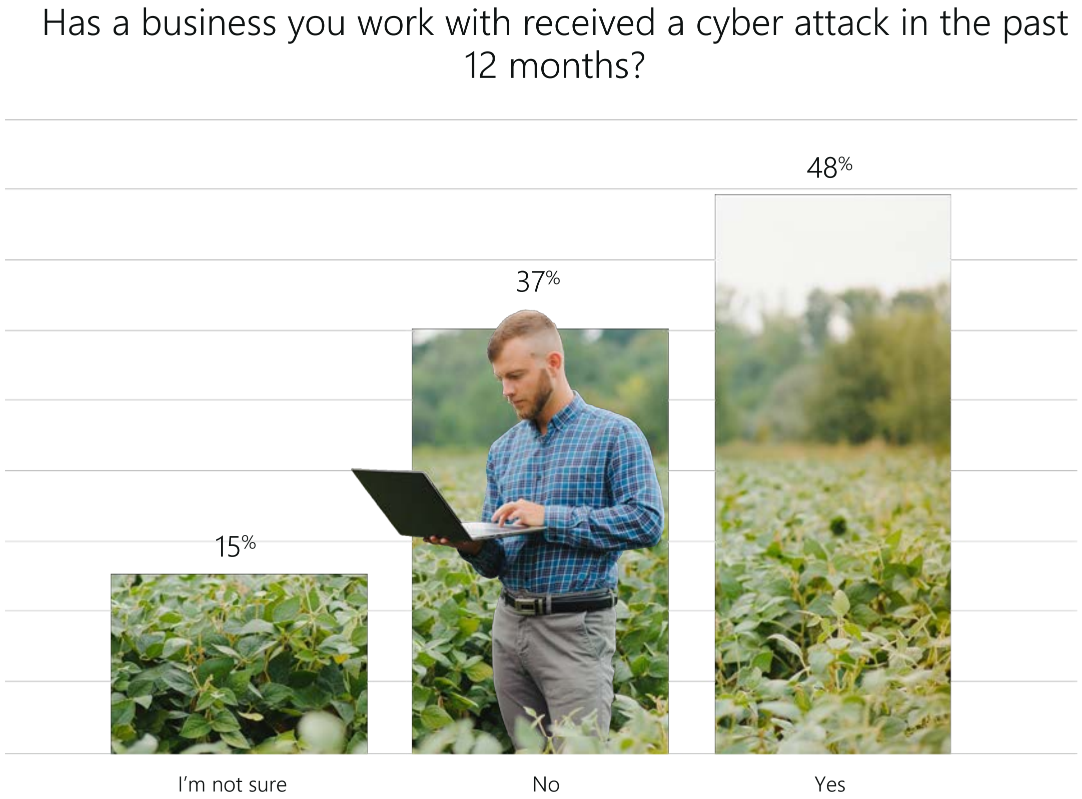
Overall, how would you describe the impact of this cyber attack?



Of those who have had a cyber attack

Type of cyber attack





Cyber security plan

Do you currently have a cyber security plan for your farm?

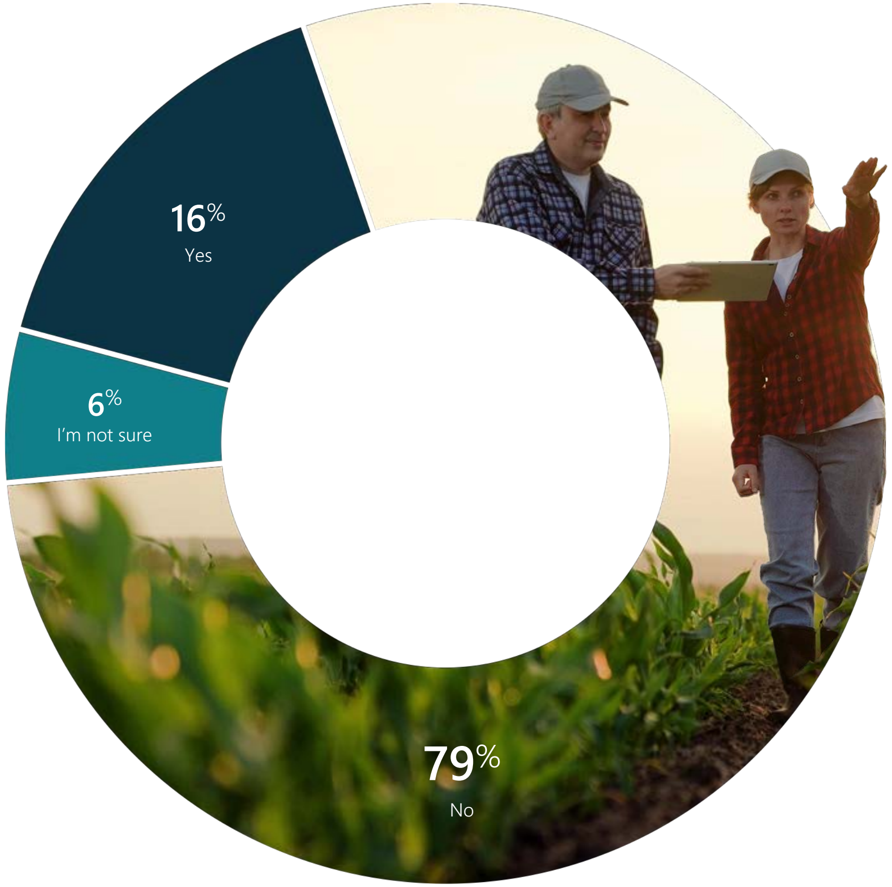
79% No

16% Yes

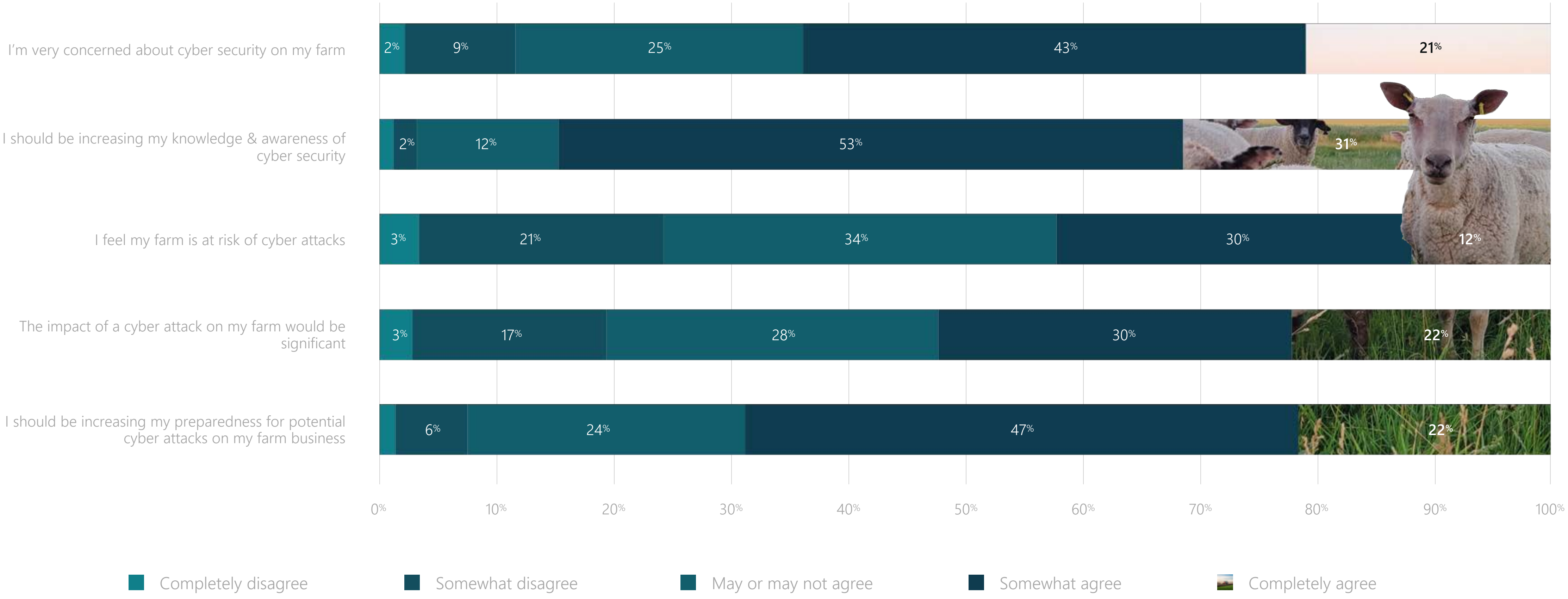
6% I'm not sure

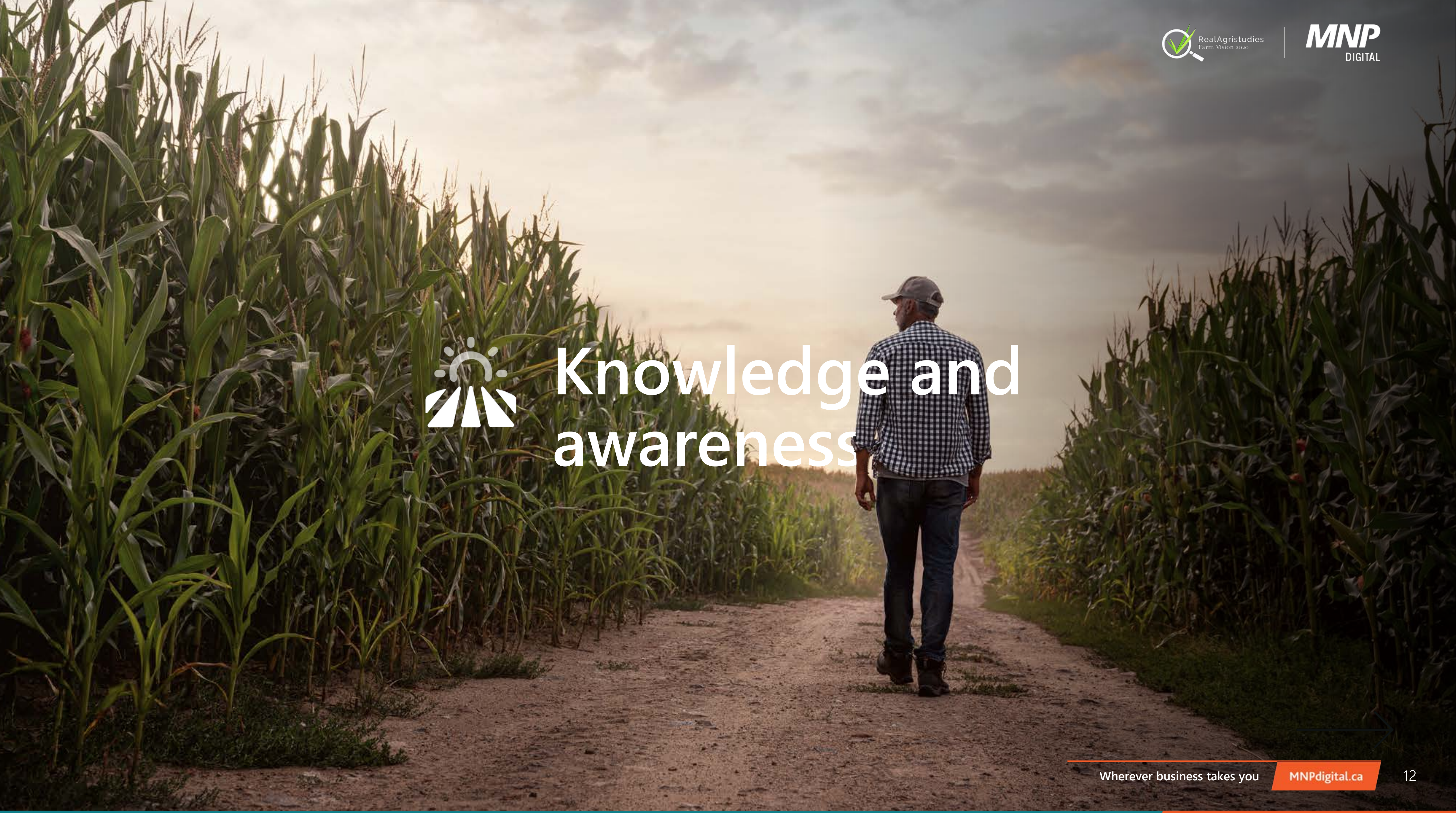
Cyber security plan

Do you currently have a cyber security plan for your farm?



Attitudes towards cyber security





Knowledge and awareness

Understanding cyber security is the first step toward safeguarding operations, yet knowledge levels among farmers vary significantly across demographics. The majority of respondents rate themselves as somewhat knowledgeable, particularly those in the 35 to 54 age range, aligning with their active use of technology in daily operations. Conversely, younger respondents (under 35) and older respondents (55 and above) were more likely to rate themselves as very knowledgeable. While this confidence may stem from familiarity with digital tools or a sense of immunity due to limited use, it can sometimes translate into overconfidence — leaving blind spots for attacks.

Interestingly, farm size and income levels also correlate with self-assessed knowledge. Smaller farms report the lowest levels of cyber security awareness, likely due to limited resources and lack of dedicated IT support. Larger operations, with greater technological investments, often prioritize cyber security training and infrastructure. However, even among these groups, complacency can pose a challenge. Overconfidence, as seen in phishing tests conducted in other industries, often leads to lapses in judgment and can make even the most senior personnel vulnerable to attacks.

The divide between knowledge and confidence among different demographics reveals the importance of targeted education. Younger farmers, while adept at navigating technology, may not fully grasp the complexity of modern cyber threats. Older farmers, on the other hand, may underestimate their exposure due to limited reliance on digital systems, with a more traditional standpoint, or a lack of awareness. Bridging this gap requires straightforward, accessible training resources that address common vulnerabilities such as phishing, ransomware, and social engineering.

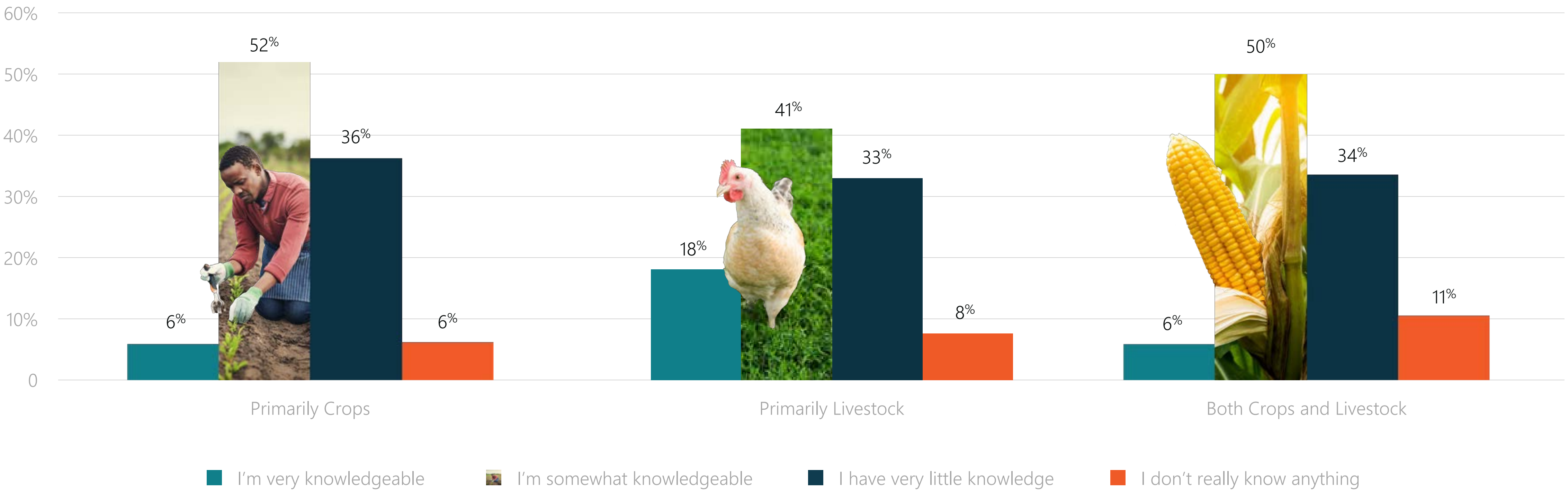
Ultimately, raising awareness across all age groups and farm sizes is essential to mitigating risks. Cyber security is not just about awareness but also about vigilance and preparedness. As noted by MNP's Cyber Security Lead, Eugene Ng, it's key to focus on the 80/20 rule — meaning that 80 percent of risks can be reduced by addressing 20 percent of the most common vulnerabilities. For farmers, it's about adopting simple yet effective practices like verifying communications, using secure passwords, and regularly updating systems. Awareness combined with actionable steps can create a more resilient agricultural sector.

80/20

Rule

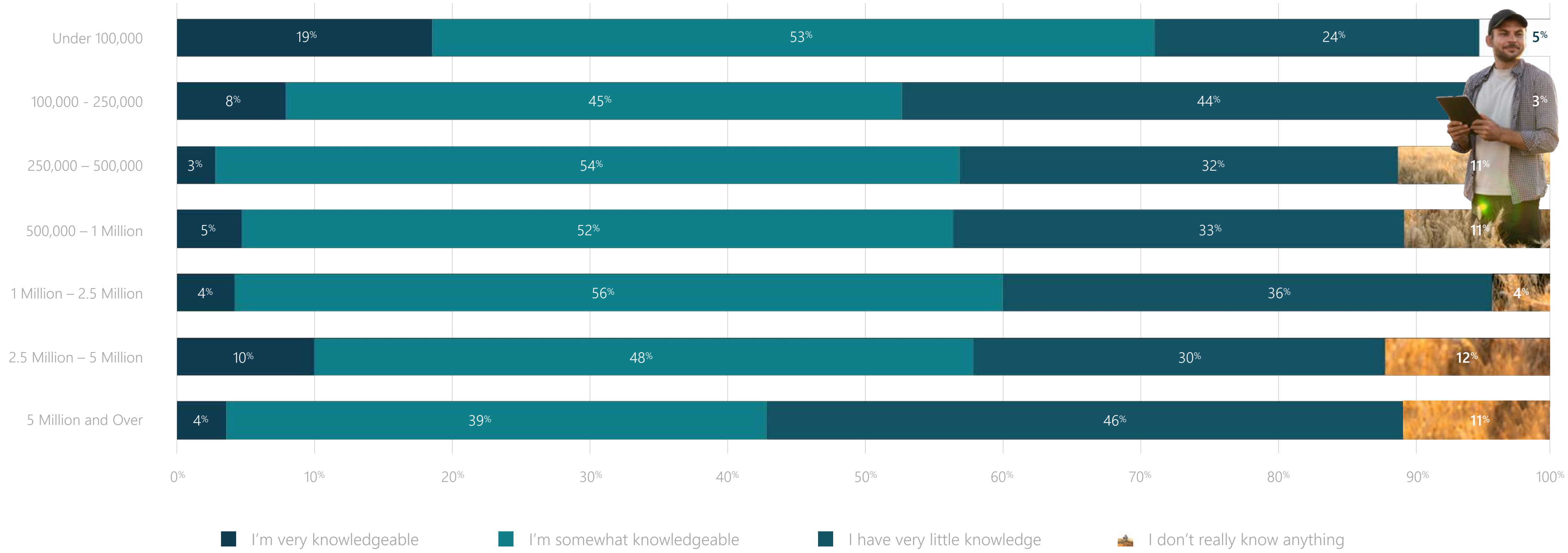
Knowledge & awareness of cyber threats *By farm type*

How would you rate your overall level of knowledge and awareness of cyber security and the threats they possess?



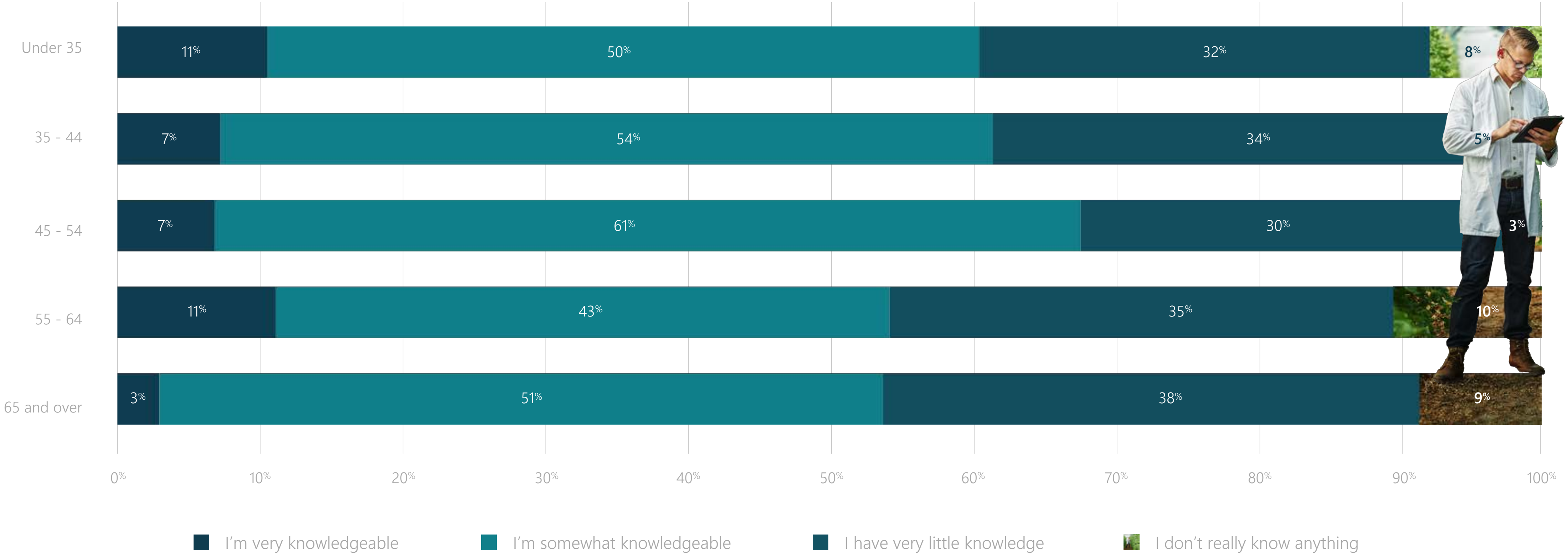
Knowledge & awareness of cyber threats *By farm size (income)*

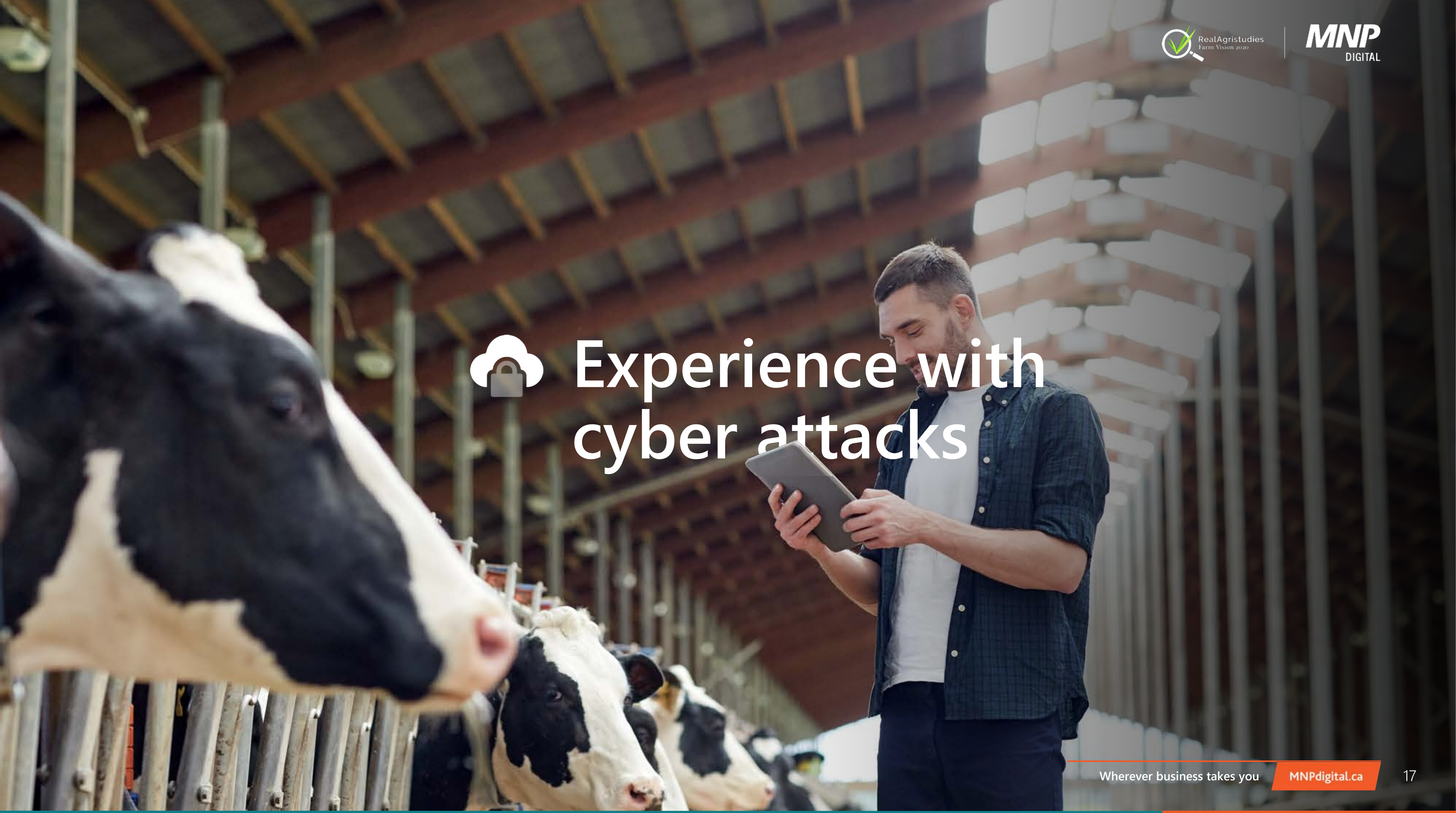
How would you rate your overall level of knowledge and awareness of cyber security and the threats they possess?



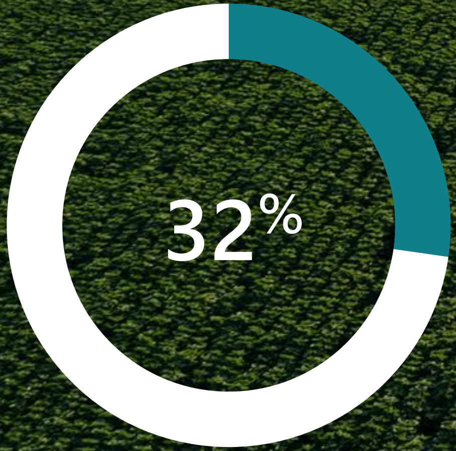
Knowledge & awareness of cyber threats *By age category*

How would you rate your overall level of knowledge and awareness of cyber security and the threats they possess?





Experience with cyber attacks



Younger respondents under 35 report the lowest incidence of attacks (5%), while the highest rates are among larger farms earning over $5 million annually, where 32 percent have been targeted.

Cyberattacks remain an underreported issue within the agricultural sector. According to the survey, only nine percent of respondents believe their farm has been targeted by a cyberattack. However, this low figure likely reflects a lack of awareness rather than reality. Many attacks — such as phishing and business email compromise — are designed to be subtle, leaving victims unaware that they've been breached. This highlights a dangerous void in detection and reporting, especially among farmers who may not have the tools or training to identify these threats.

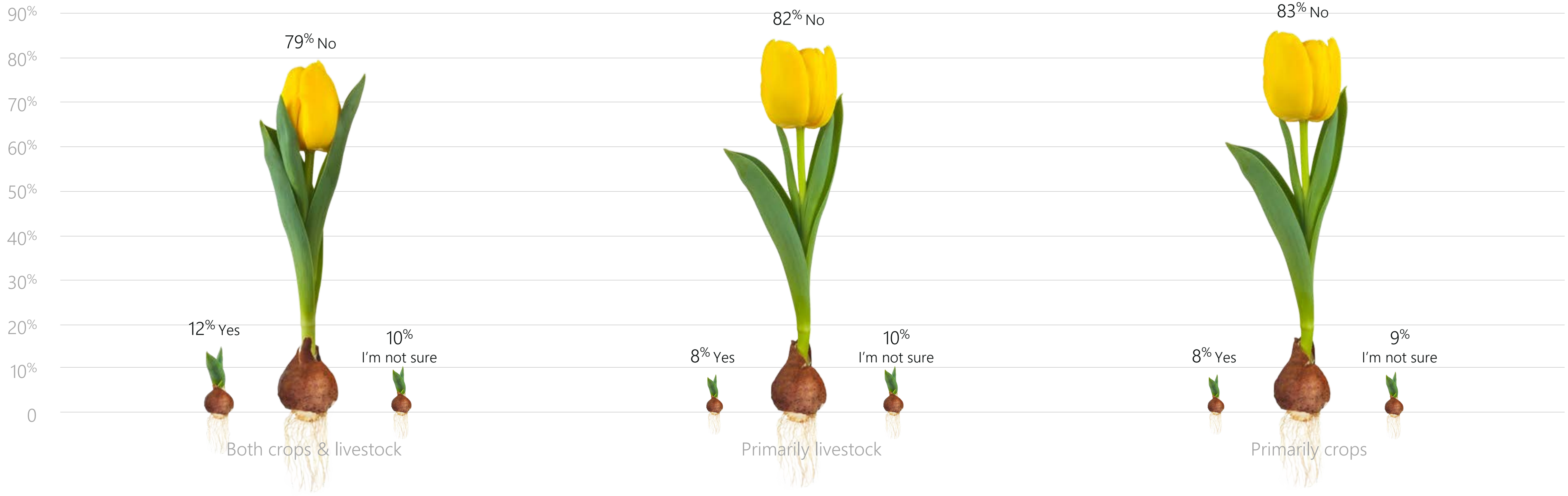
The data reveals intriguing demographic trends in cyberattack experiences. Younger respondents under 35 report the lowest incidence of attacks (5%), while the highest rates are among larger farms earning over $5 million annually, where 32 percent have been targeted. Unsurprisingly, this disparity suggests that larger farms, with more extensive digital footprints and financial assets, are more attractive to threat actors. Meanwhile, smaller farms and younger farmers may be less targeted, but they also may not recognize the signs of a breach. This disconnect poses a risk, as many cyberattacks, particularly social engineering, prey on human error and often go unnoticed.

Farm type also plays a role in cyberattack vulnerability. Farms focused on both crops and livestock reported slightly higher rates of attacks compared to those specializing in just one area. This may be due to the broader range of operational technologies involved in their operations, such as livestock monitoring systems and crop management tools. Operational technologies are often overlooked in cyber security planning, leaving them vulnerable to breaches that could disrupt imperative systems, from automated feeding to ventilation.

These findings underscore the need for proactive measures. Farmers must prioritize cyber security awareness and incident response planning. Simple steps— like implementing regular training to recognize phishing attempts, verifying financial transactions, and maintaining offline backups — can significantly mitigate risks. Larger farms, often the prime targets, should allocate resources toward dedicated cyber security teams or external IT support. For smaller farms, leveraging free resources like Cybersecure Canada provides a cost-effective starting point. Cyber security is no longer optional, but a vital component of safeguarding the agricultural sector and its essential role in our economy.

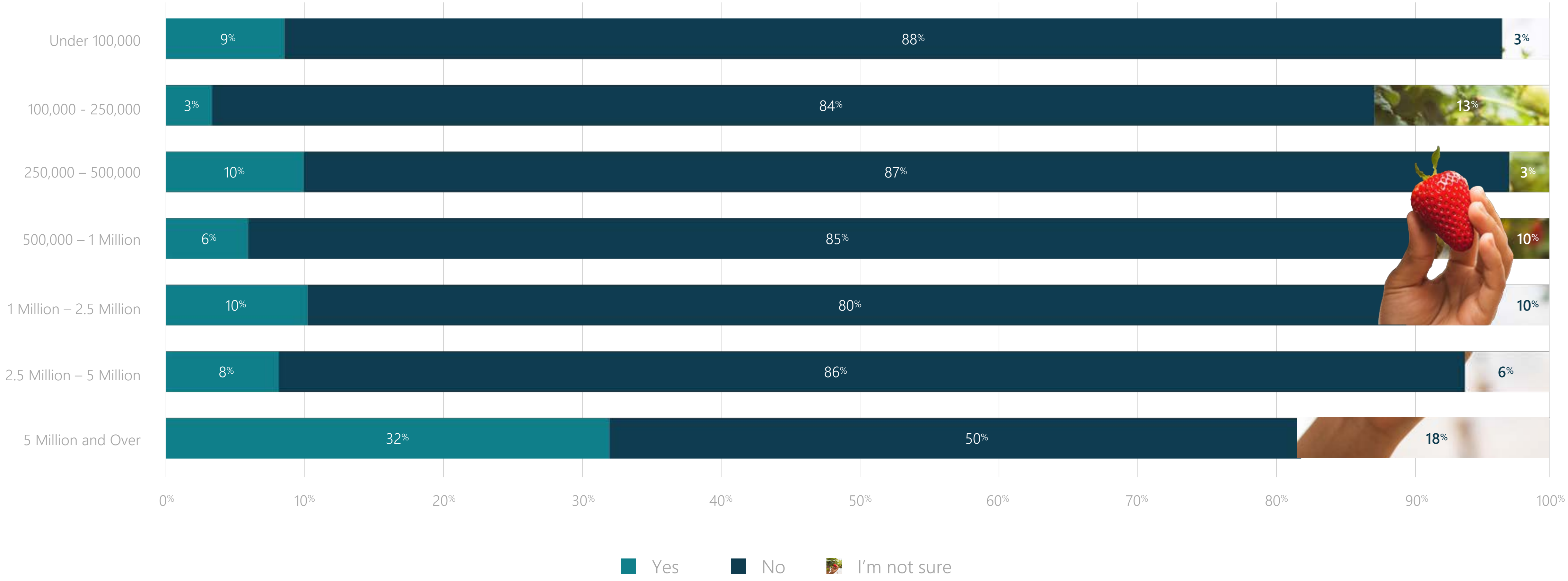
Experience with cyber attacks *By farm size*

Has your farm ever received a cyber attack?



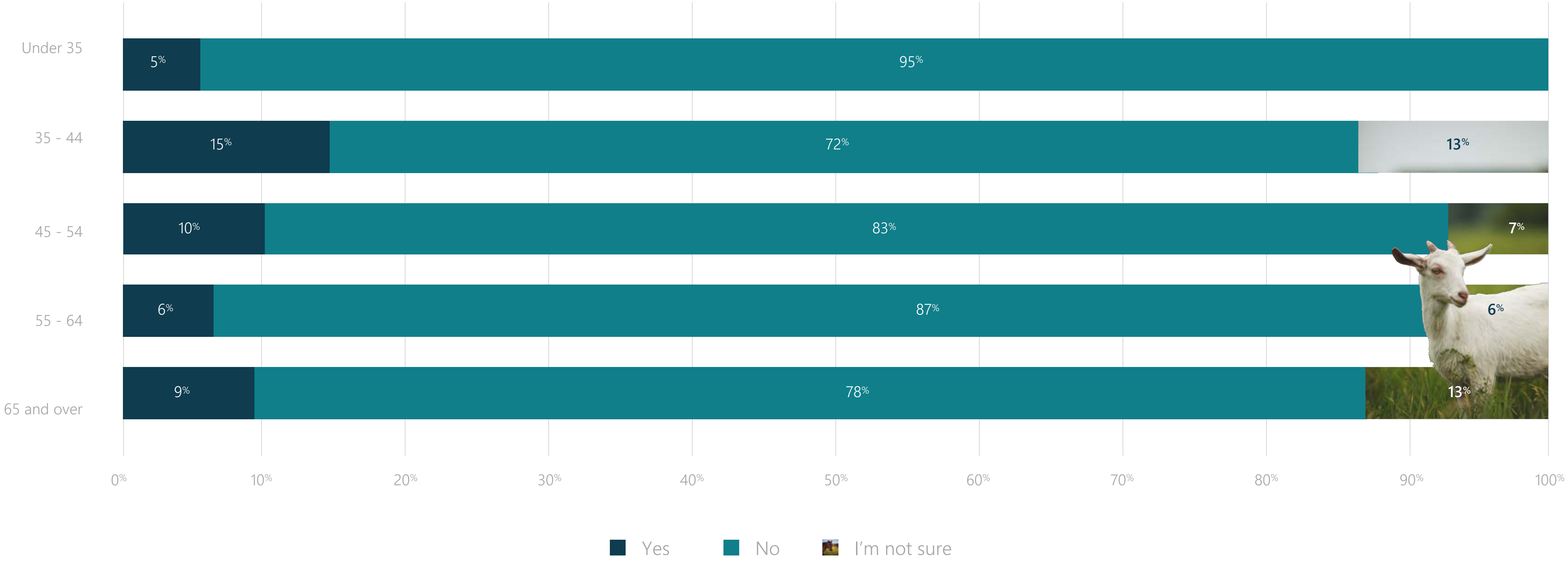
Experience with cyber attacks *By farm size (income)*

Has your farm ever received a cyber attack?



Experience with cyber attacks *By age category*

Has your farm ever received a cyber attack?



Cyber security planning

The findings of the survey reveal a disconnect in cyber security planning across the agricultural sector. Alarmingly, only 16 percent of respondents reported having a cyber security plan in place for their operations. This lack of preparedness leaves farms vulnerable to the increasingly sophisticated cyber threats targeting operational technology — the systems that control essential farm functions like irrigation, feeding, and climate control. Cyberattacks are not a question of if but when, and without a plan in place, farms risk operational disruption, financial losses, and even threats to human and livestock safety.

Cyber security planning varies significantly by farm size and income. Farms generating over $2.5 million annually are more likely to have implemented cyber security measures, likely due to greater resources and their reliance on complex technological systems. In contrast, smaller farms earning less than $250,000 annually report the lowest levels of cyber security planning, with many respondents likely underestimating their exposure to threats. This disparity highlights the need for scalable and accessible solutions tailored to smaller farms, which often lack the resources to implement comprehensive cyber security measures.

Age demographics also reveal notable trends. Younger farmers under 35 are the most proactive, with 19 percent reporting that they have a cyber security plan. This group's higher familiarity with technology may contribute to their preparedness. However, farmers aged 35-44 reported the lowest levels of planning, with just nine percent having a cyber security plan in place. This mid-range demographic may be caught between the rapid adoption of technology and a lack of resources or training to address emerging risks. Targeted education campaigns could bridge this gap, emphasizing the importance of even basic steps like incident response plans, data backups, and phishing awareness.

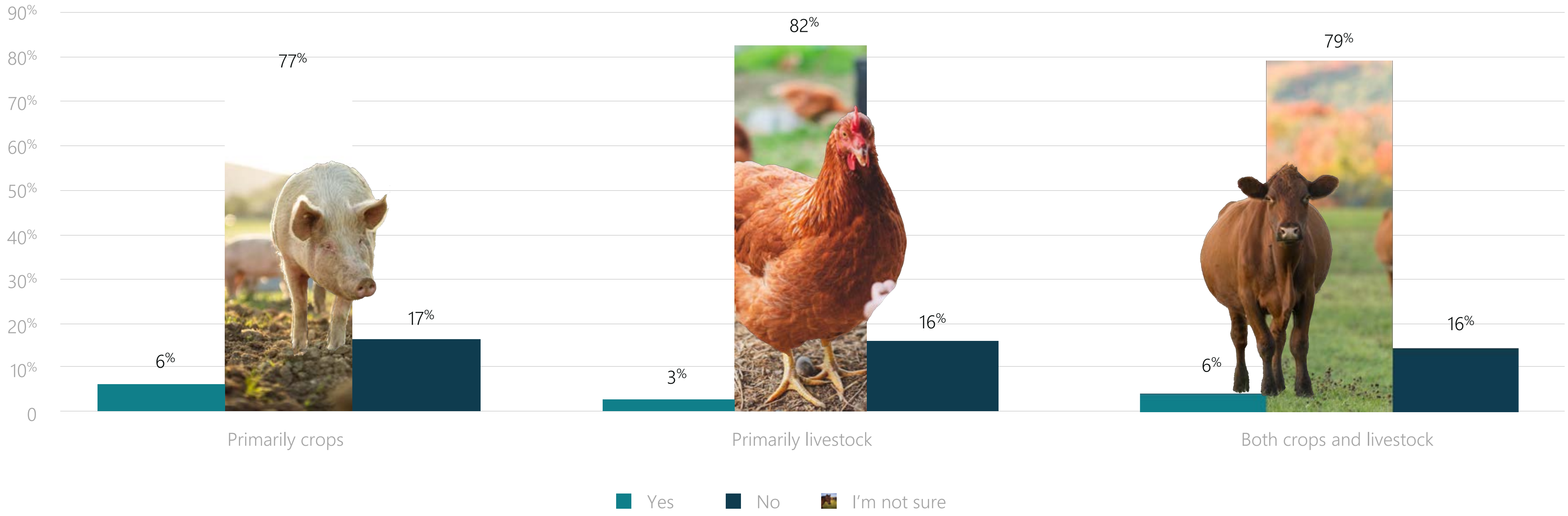
The survey underlines the urgent need for widespread adoption of cyber security planning in agriculture. Farms must view cyber security as integral to their operations, not an optional expense. Fortunately, getting started is very straightforward and a plan is something all farms can rapidly implement. The key to minimizing risks is to focus on simple yet impactful measures — ensuring primary systems are protected, employees are trained, and response plans are in place. Proactive preparation not only reduces vulnerabilities but also ensures that farms can maintain operational resilience in an increasingly connected world.

16%

reported having a cyber security plan in place

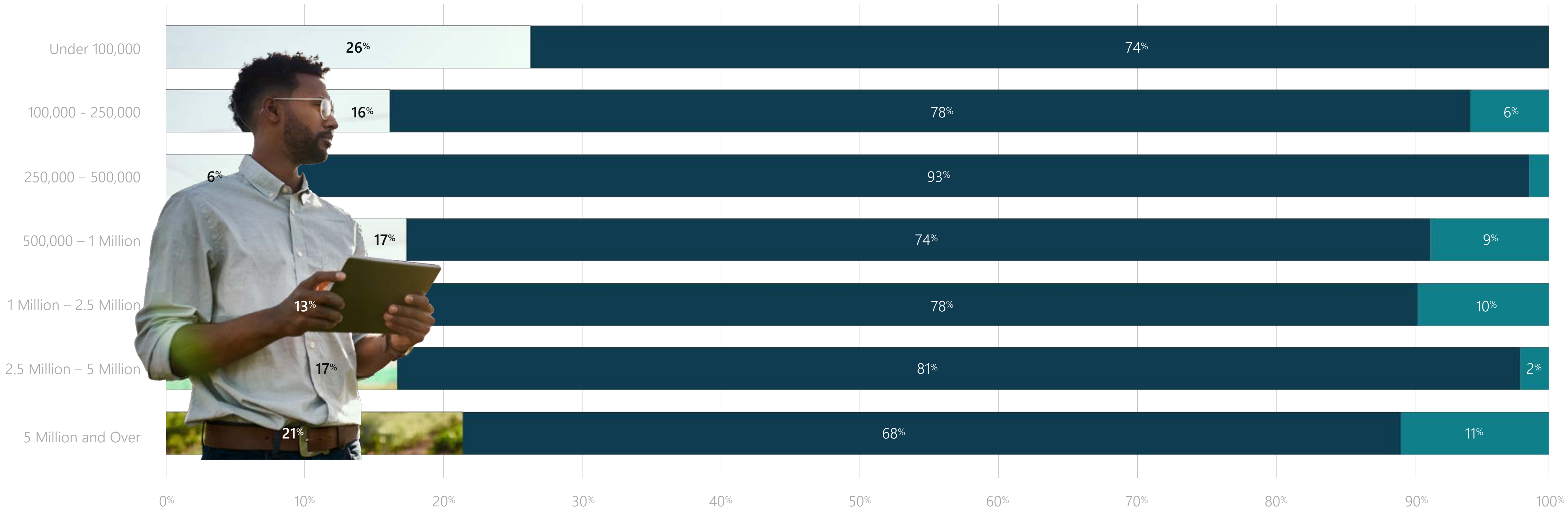
Cyber security plan *By farm type*

Do you currently have a cyber security plan for your farm?



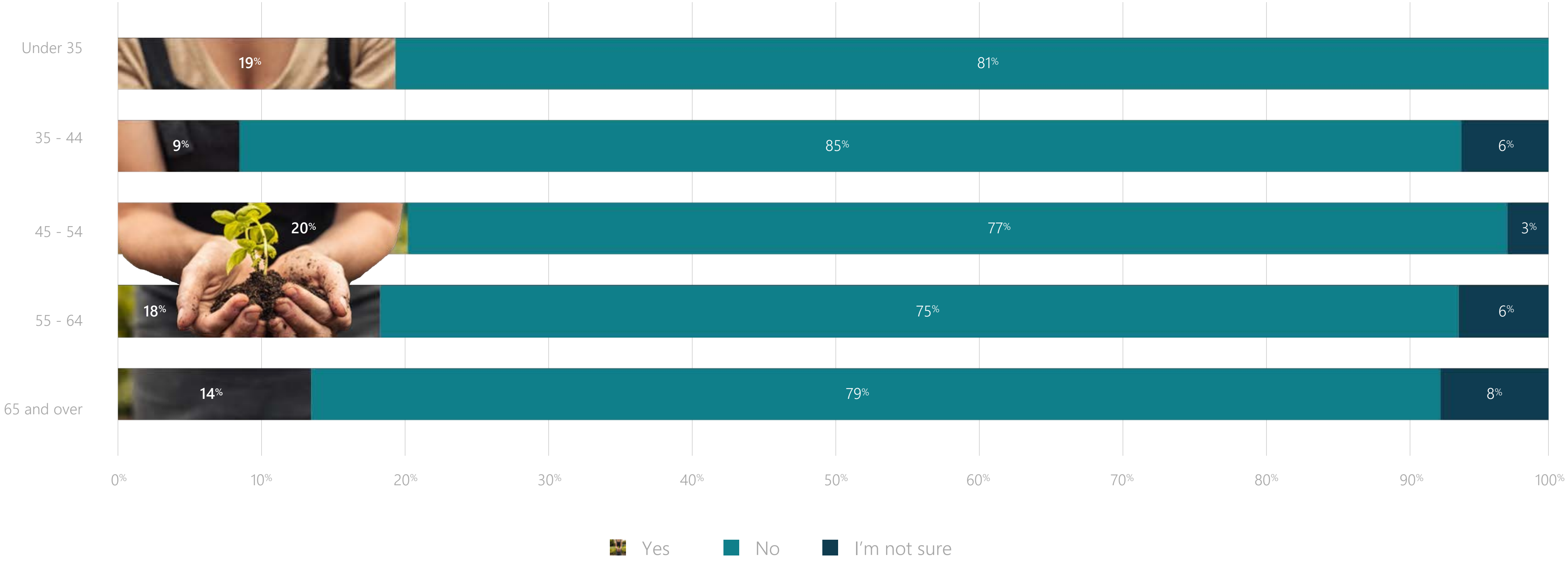
Cyber security plan *By farm size (income)*

Do you currently have a cyber security plan for your farm?



Cyber security plan *By age category*

Do you currently have a cyber security plan for your farm?



Attitude statements

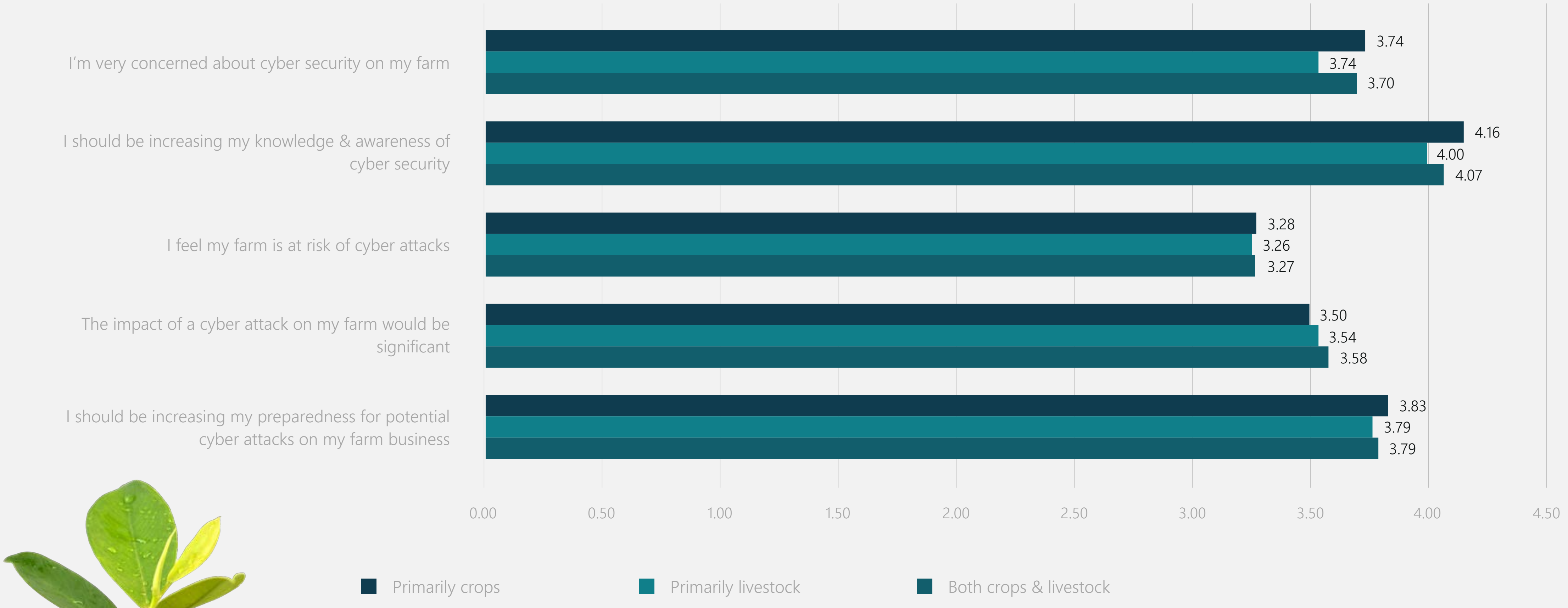
The survey highlights varying attitudes toward cyber security, shaped by farm type, income, and age group. While farmers broadly agree on the importance of improving their knowledge, their perceptions of risk and readiness differ. Farmers managing both crops and livestock showed slightly higher concern levels, likely due to their reliance on a broader range of operational technologies (OT), such as automated feeding systems and irrigation controls. These technologies, while essential, are often overlooked in cyber security planning, leaving essential operations vulnerable to attack.

Income levels reveal further contrasts. Larger farms with revenues exceeding $2.5 million expressed the highest concern, driven by their reliance on advanced technology and exposure to larger-scale risks. Similarly, smaller farms with revenues under $100,000 demonstrated significant concern, recognizing that even a minor attack could be devastating. Mid-sized farms, however, showed less concern, potentially underestimating their risks. Overconfidence among this group, coupled with rapid digital adoption, may leave openings in their defenses.

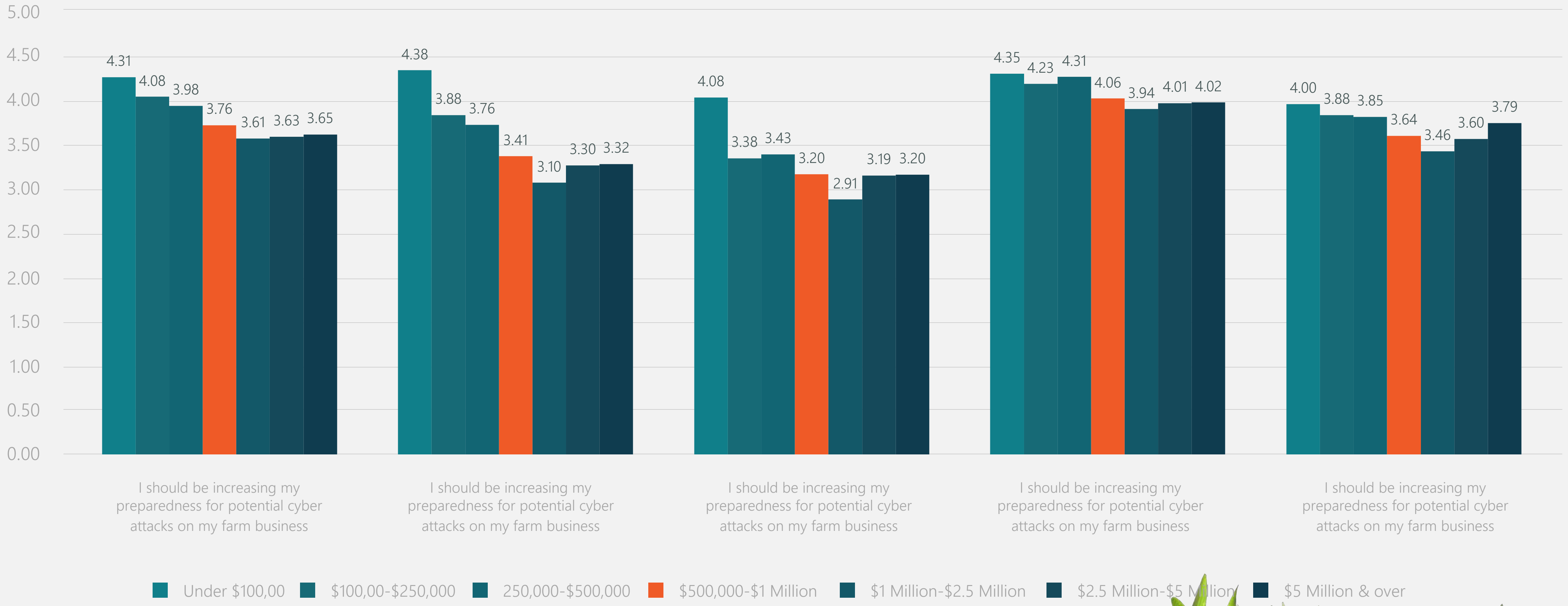
Age demographics add another layer of insight. Farmers aged 35 to 54 were most likely to acknowledge the need for better preparedness, reflecting their active use of technology in operations. Younger farmers (under 35) displayed confidence in their technical abilities but acknowledged gaps in planning — a dynamic that can result in overlooked vulnerabilities. Older farmers (65 and over) expressed balanced levels of concern, reflecting a mix of caution and reliance on legacy systems. These generational differences highlight how familiarity with technology shapes cyber security priorities and preparedness.

Despite widespread acknowledgment of the risks, few farmers have implemented comprehensive cyber security measures. Practical, tailored solutions — such as response plans, targeted training, and protection for OT systems — are pivotal to turn concern into action. By addressing these gaps and equipping farms with accessible resources, the agricultural sector can take proactive steps to defend against increasingly sophisticated cyber threats.

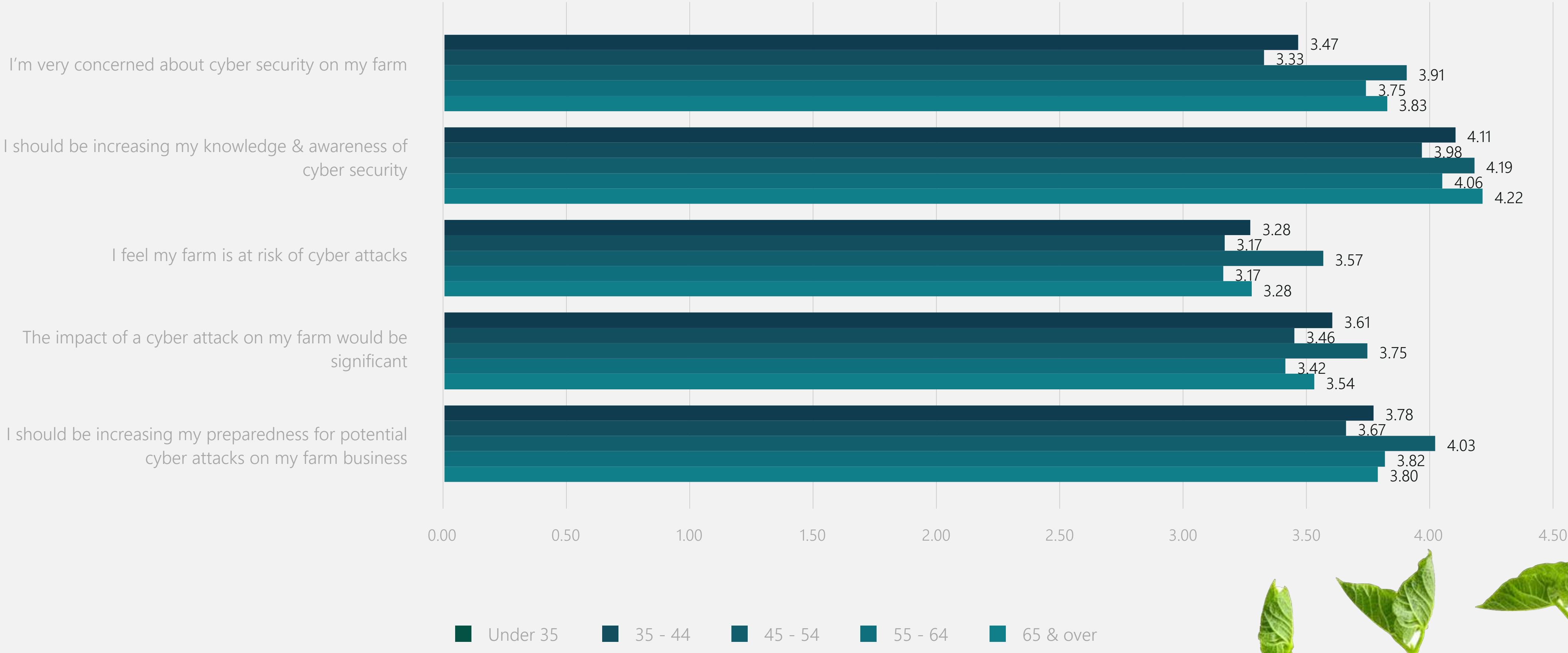
Attitude statements *By farm type*



Attitude statements *By farm size (income)*



Attitude statements *By age category*

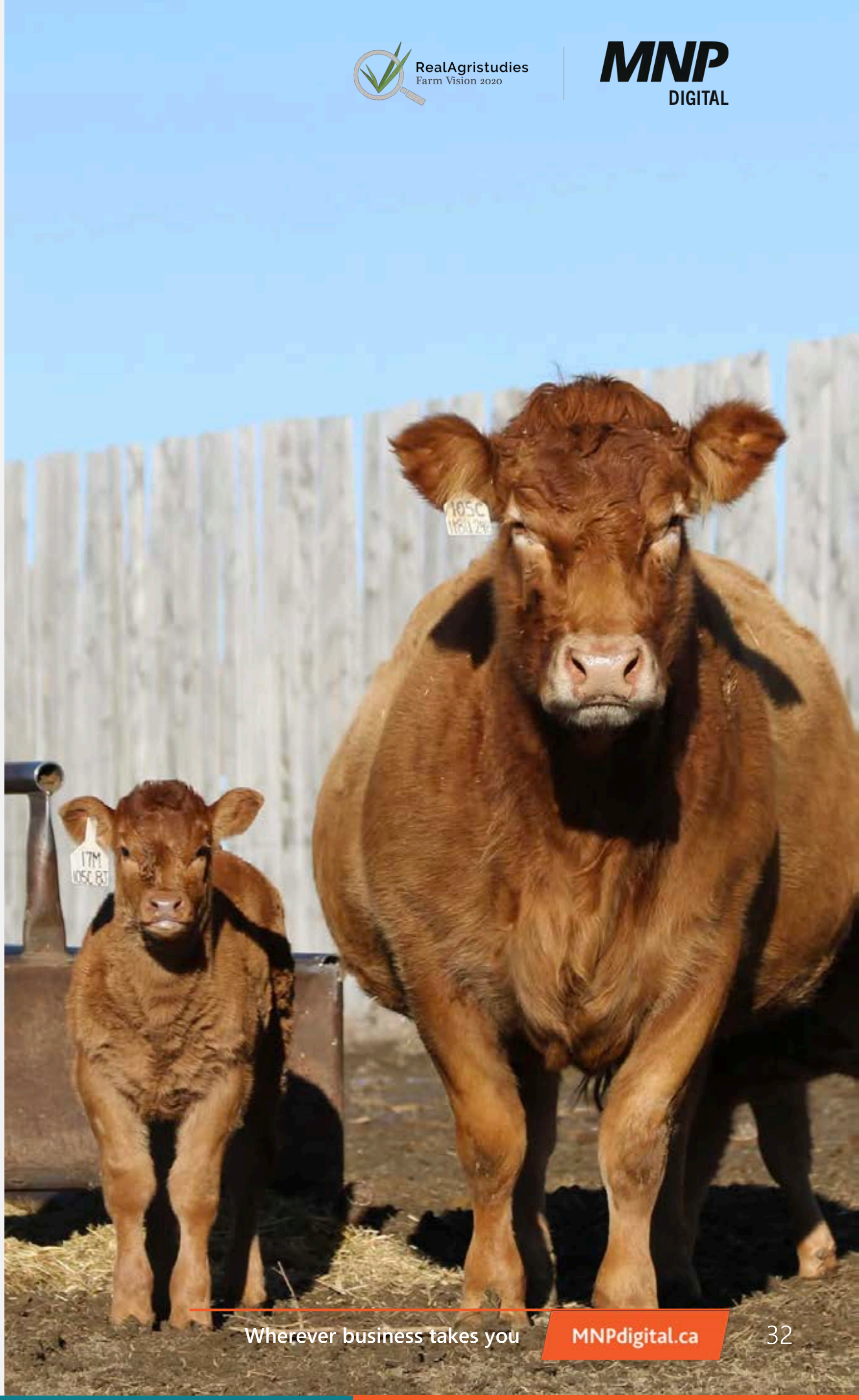


Make your next steps count

As farms adopt advanced technologies like GPS-enabled grain tractors, automated ventilation systems, and precision farming tools, cyber security has become an essential consideration. Recent research demonstrates how even everyday devices, such as household vacuum robots, can be exploited to manipulate their behavior. In the agricultural context, this could translate to disruptions in critical systems — imagine a grain tractor's GPS being manipulated to plant off-course or an automated ventilation system failing to regulate air in a livestock barn. These scenarios highlight how technology designed to improve efficiency can also introduce risks when left unprotected.

At the same time, cybercriminals are becoming increasingly sophisticated in their tactics. Farmers may not only face threats to their equipment but also to their decision-making. A phishing email appearing to come from a trusted supplier could request an urgent payment or sensitive information. These scams rely on human error and trust, making them especially effective in a fast-paced farming environment where attention is divided. The good news is that with education, awareness, and some proactive steps, farms can mitigate these risks and stay ahead of the curve.

At MNP, we have deep roots in the agriculture industry and are here to help farmers navigate this evolving landscape. Farming is the cornerstone of our communities and Canada's food system. By focusing on practical measures, such as securing operational technology, increasing team awareness of cyber scams, and creating response plans, farmers can protect their operations while embracing the benefits of innovation. With a clear path forward, you can build resilience and confidence for the future. Let's work together to safeguard your farm — connect with us to explore the resources and support available to you.



Additional free resources

- Canadian government cyber security information: https://www.cyber.gc.ca/
- Canadian government agriculture cyber security information: https://agriculture.canada.ca/en/programs/tools-manage-farm-risk-and-finance/cyber-security-and-your-farming-business
- Education courses: https://www.cyber.gc.ca/en/education-community/learning-hub/courses
- Reporting a cyber incident: https://www.cyber.gc.ca/en/incident-management

Eugene Ng
Partner, Cyber Security Lead
eugene.ng@mnp.ca

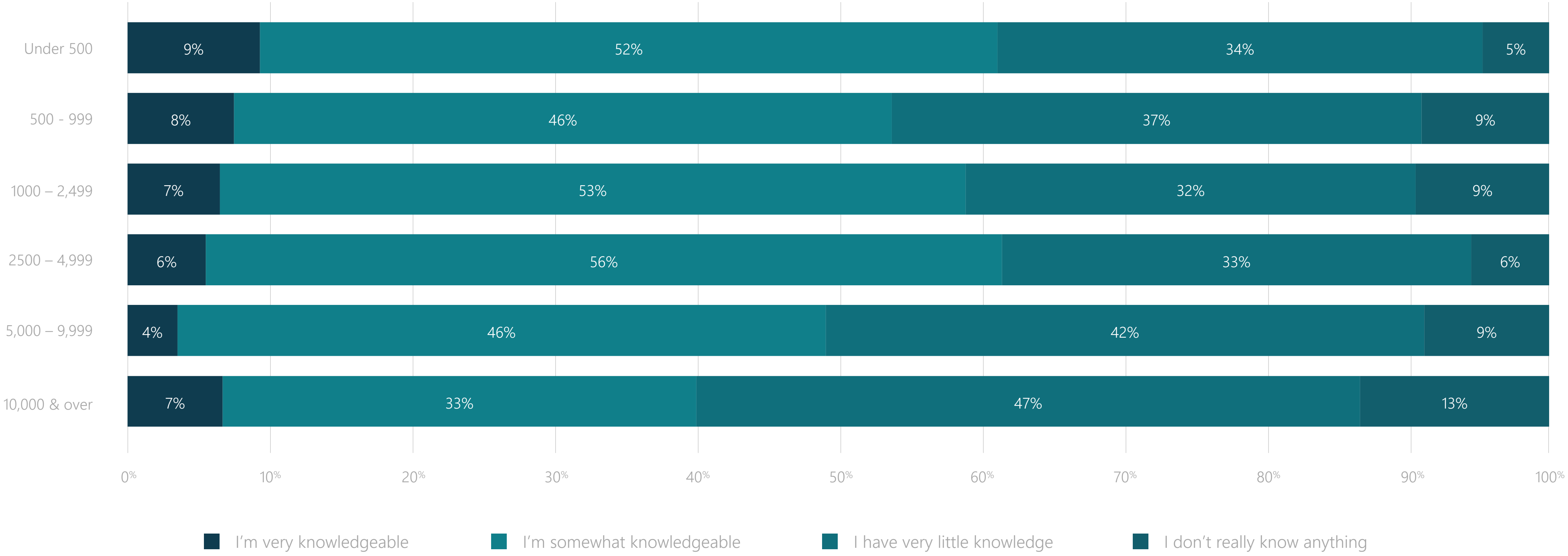
Curtis Adair
Partner, Digital Advisory
curtis.adair@mnp.ca

John McLaughlin
Partner, Client Services
john.mclaughlin@mnp.ca

Appendix

Knowledge & awareness of cyber threats *By farm size (acres)*

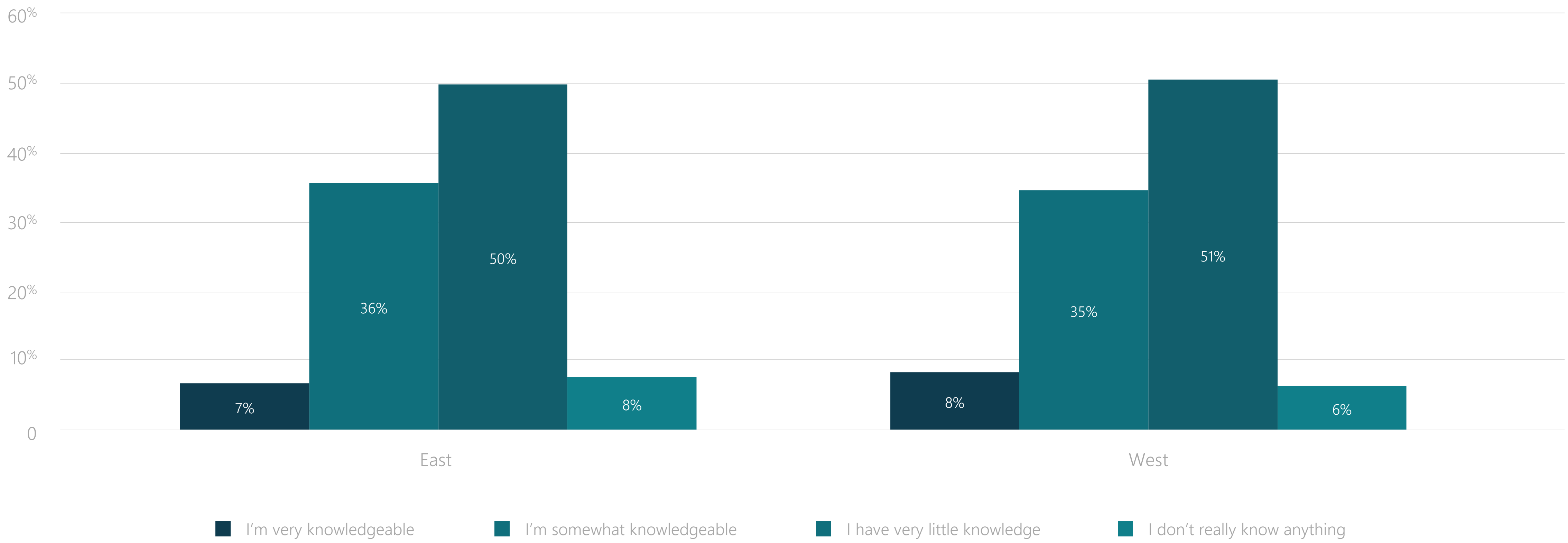
How would you rate your overall level of knowledge and awareness of cyber security and the threats they possess?



Section: Appendix

Knowledge & awareness of cyber threats *By region*

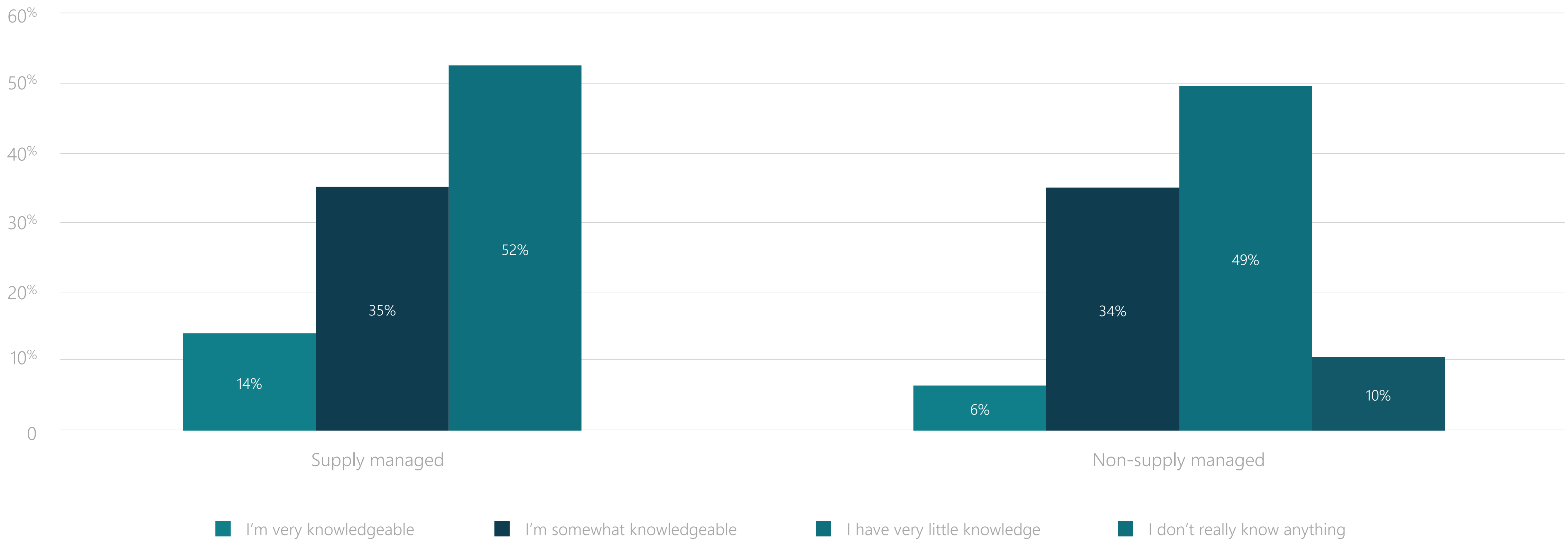
How would you rate your overall level of knowledge and awareness of cyber security and the threats they possess?



Section: Appendix

Knowledge & awareness of cyber threats *By supply managed*

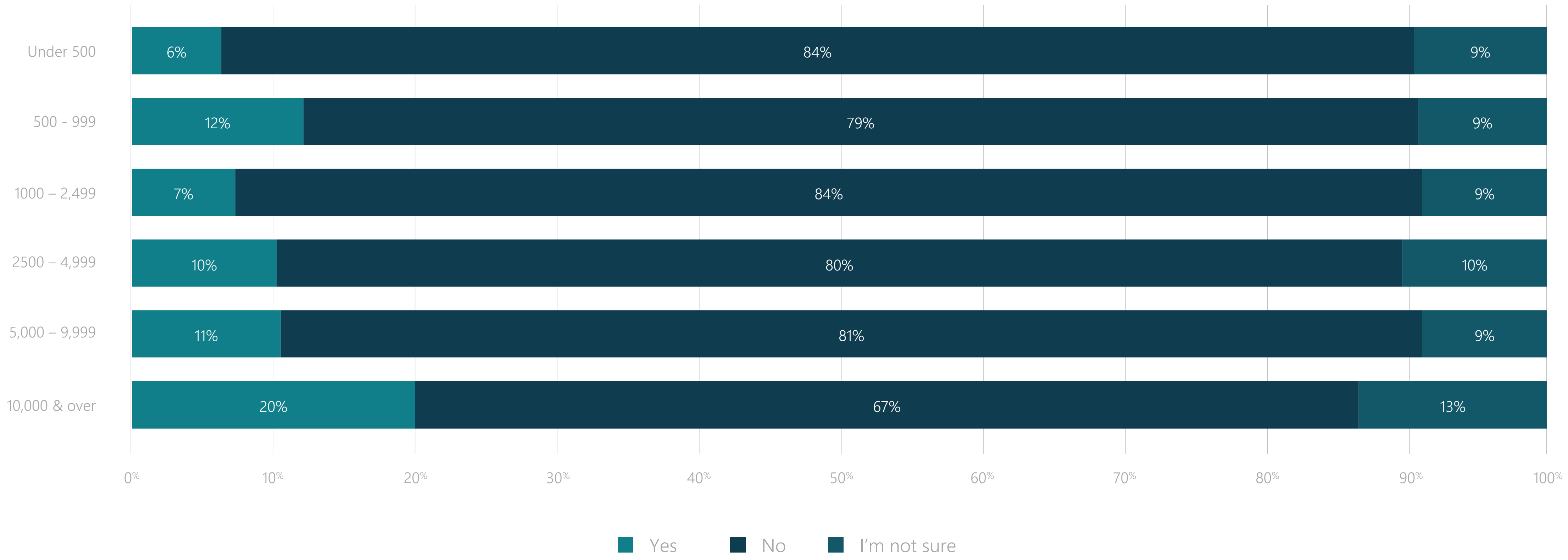
How would you rate your overall level of knowledge and awareness of cyber security and the threats they possess?



Section: Appendix

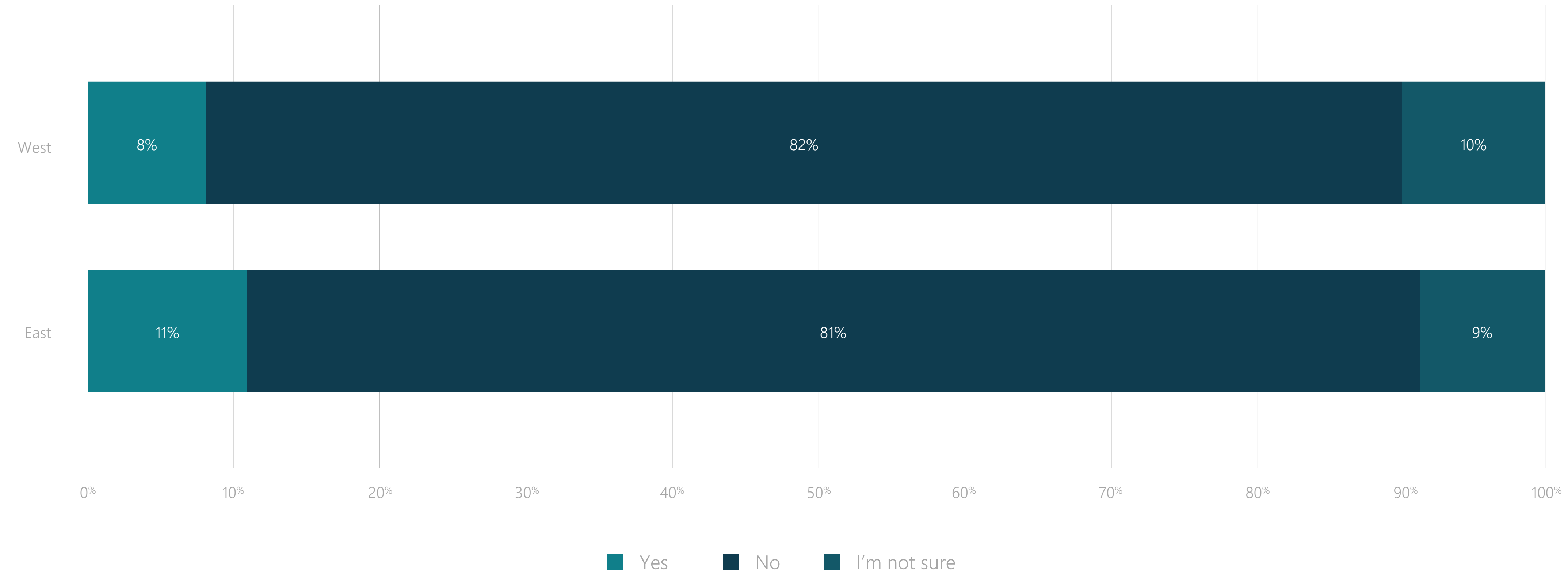
Experience with cyber attacks *By farm size (acres)*

Has your farm ever received a cyber attack?

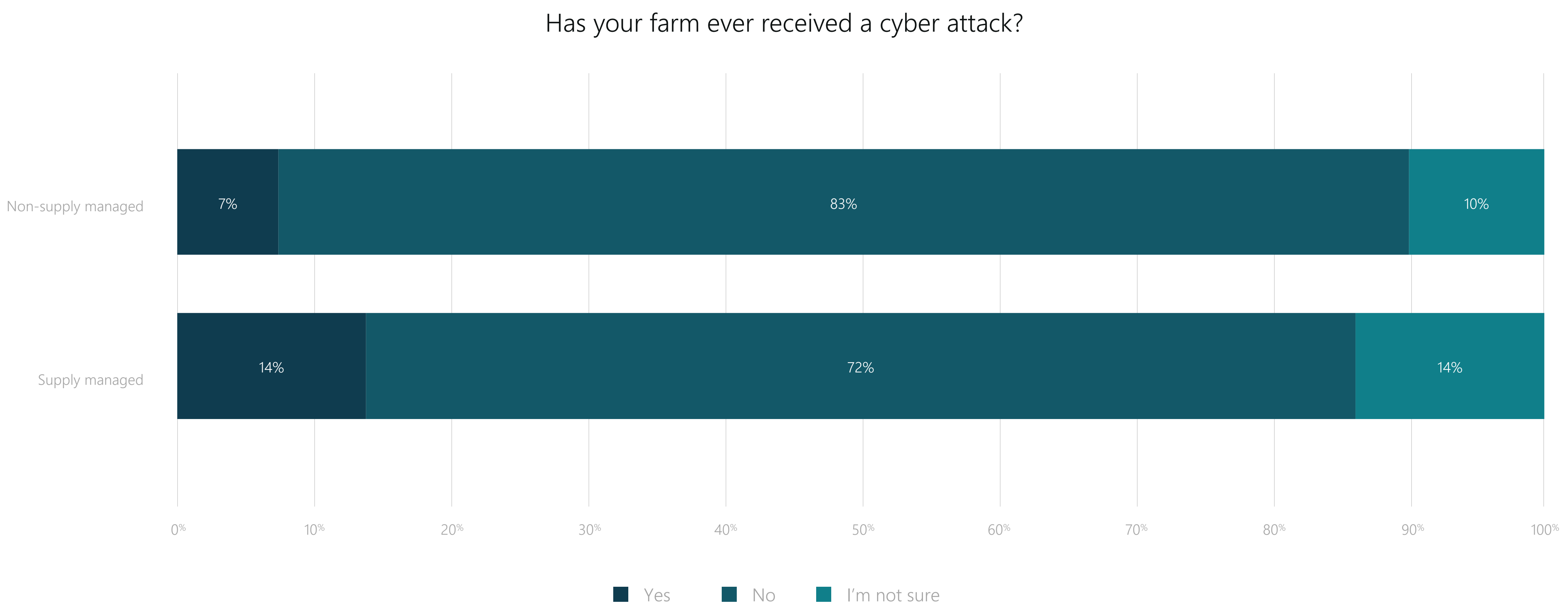


Experience with cyber attacks *By region*

Has your farm ever received a cyber attack?

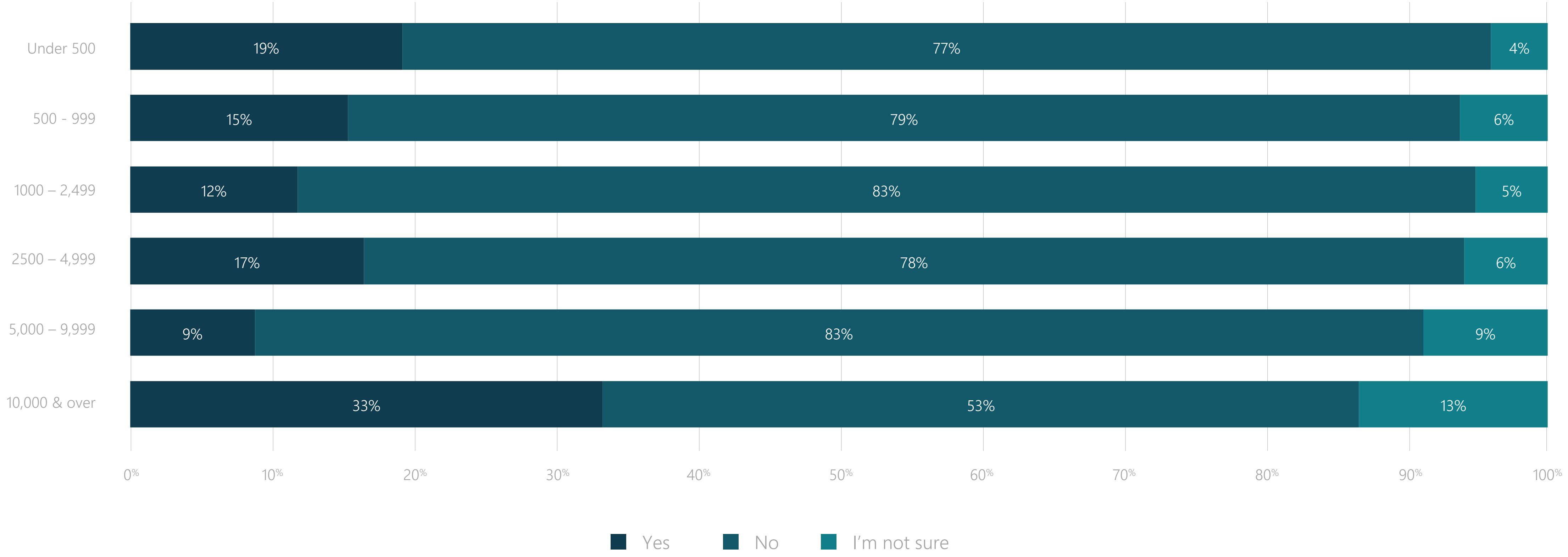


Experience with cyber attacks *By supply managed*



Cyber security plan *By farm size (acres)*

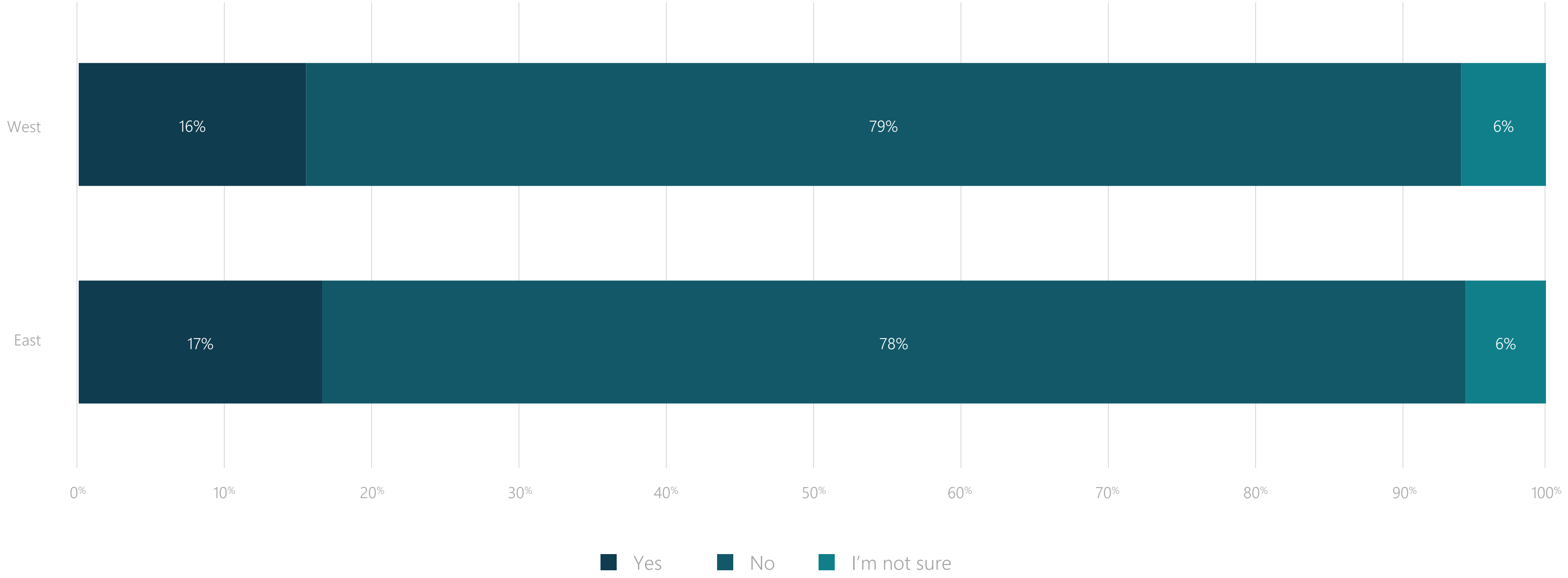
Do you currently have a cyber security plan for your farm?



Section: Appendix

Cyber security plan *By region*

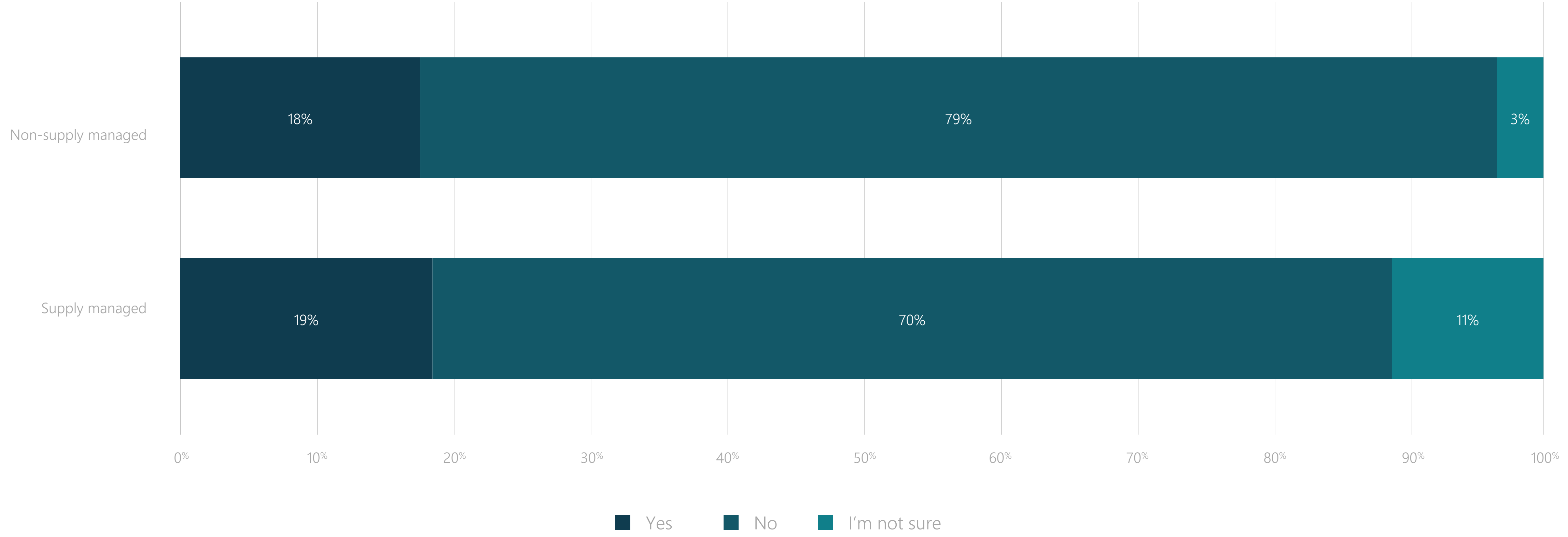
Do you currently have a cyber security plan for your farm?



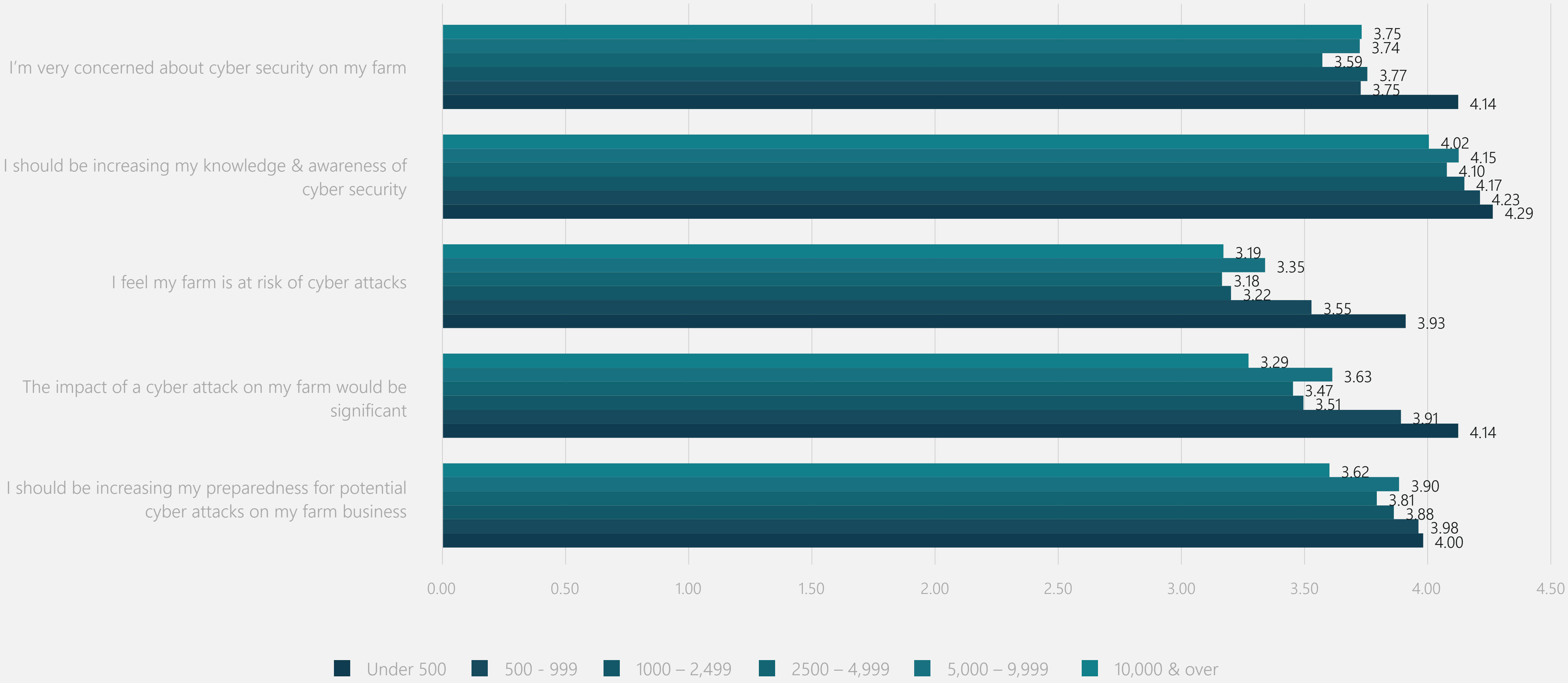
Section: Appendix

Cyber security plan *By supply managed*

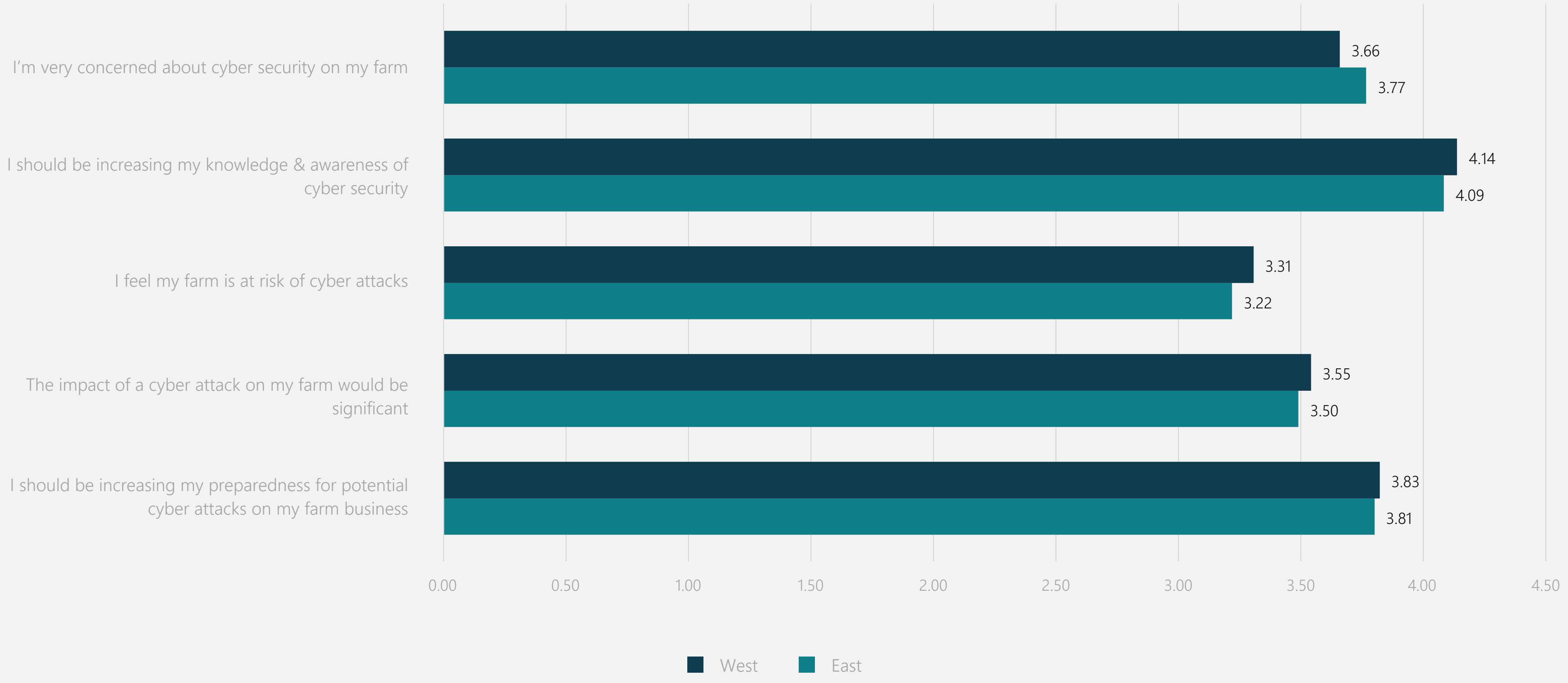
Do you currently have a cyber security plan for your farm?



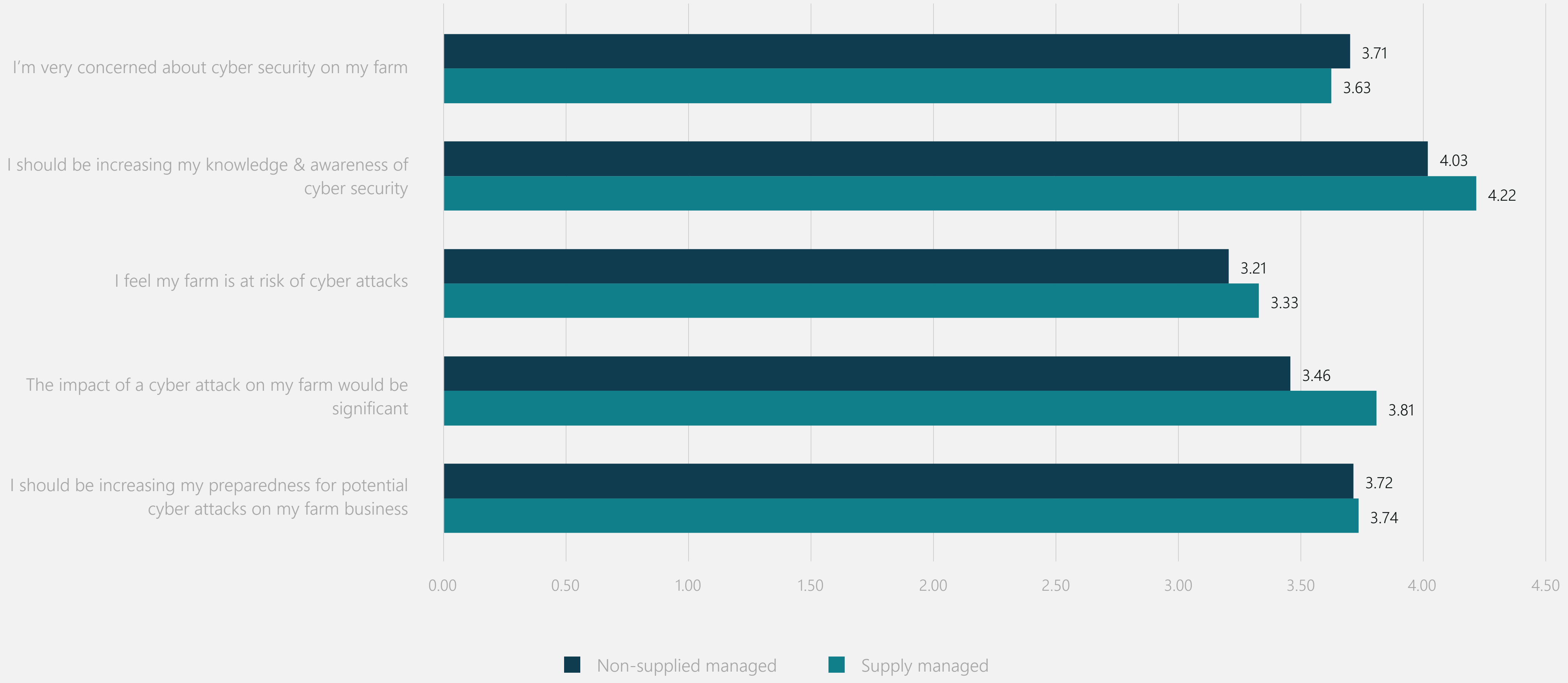
Attitude statements *By farm size (acres)*



Attitude statements *By region*



Attitude statements *By supply managed*



Statement	Non-supplied managed	Supply managed
I'm very concerned about cyber security on my farm	3.71	3.63
I should be increasing my knowledge & awareness of cyber security	4.03	4.22
I feel my farm is at risk of cyber attacks	3.21	3.33
The impact of a cyber attack on my farm would be significant	3.46	3.81
I should be increasing my preparedness for potential cyber attacks on my farm business	3.72	3.74

Research conducted by:

RealAgristudies
Farm Vision 2020

MNP
DIGITAL

Wherever business takes you MNPdigital.ca