‘Cyber security and data breach are not an IT issue’

Editorial, 15 November 2022

Agribusiness Australia Directors

Patrick McClelland and David McKeon

These issues should be addressed as board and executive-level governance priorities, as they have the potential to halt your business’ production at best or create a long-term reputational and even existential issue at worst.

Good governance is at the heart of any successful business, large or small. Agribusinesses leaders must consider a multitude of governance standards, from supply chain integrity, quality assurance, traceability and risk management to environmental sustainability and financial performance.

Yet, until the last few months, cybersecurity and data security were not front of mind. Recent data breaches from Optus and Medibank have changed that.

Millions of Australians have had their details accessed, with “Russian hackers” dumping private information on the “dark web”. This has drawn scrutiny from Governments, regulators, consumers, and shareholders.

Ransomware operators in particular are becoming more targeted in their attacks, focusing on businesses that hold sensitive data such as financial or health records, or businesses that cannot afford down-time.

The numbers are daunting, especially when you consider that most notifiable breaches go through to the keeper without making the news.

The number and sophistication of cyber threats in Australia continues to rise, making secondary crimes like extortion, espionage, and fraud easier to replicate at scale. The Australian Cyber Security Centre received more than 76,000 cybercrime reports last year, 13 per cent higher from the previous financial year. This equates to one report every seven minutes.1

Agribusinesses could be forgiven for thinking higher profile targets like financial and medical institutions, and other major holders of consumer data, will protect them from being attacked.

Unfortunately, agribusiness has vulnerabilities like all other businesses.

Every agribusiness through the agri-value chain must continue to adapt their cyber strategies in line with emerging threats.

So, what do we need to worry about?

---

[1] **ACSC Annual Cyber Threat Report, July 2021 to June 2022 | Cyber.gov.au**

*Agribusiness Australia serves the Australian agribusiness sector, and our membership reflects the diversity of businesses in the sector. Our vision for the future is for a growing and thriving agricultural sector where individuals, organisations and industries can strive for, and reach, their full potential; in short, a **$300bn Australian agribusiness sector by 2030**.*

To achieve our vision we advance the interests of the Australian agribusiness sector through advocacy, promotion, and leadership, and we support our members and networks through events, services, and platforms for engagement.

As noted above, a key threat is ransomware attackers, who are targeting their victims more carefully. Food processors with dynamic demands from customers such as supermarkets and quick service restaurants, are natural targets as they need to keep operating to fulfil dynamic daily contractual obligations. Stability and continuity of supply is critical for these businesses.

Encrypting or locking up systems can threaten not only profitability but staff safety, food safety, quality assurance and supply chain traceability. They also can create massive disruption and reputational damage to an agribusiness, while imposing significant costs on the business.

Good governance not only necessitates scenario planning for such attacks but investing in and trailing new ways to redouble cyber security protocols and standards.

This means working with all employees and partners – from suppliers, advisors, and other SMEs - to ensure protocols are sophisticated and watertight as your own. Frequently, malware and ransomware reach their targets through partners such as payroll and HR software providers, who invertedly expose the organisation to the threat.

So, what can we as agribusiness leaders do about it?

Cyber security practices and policies must be updated frequently, and training and development is essential, for everyone associated with the business. Insurance policies are available and can be explored to mitigate risks to all businesses, large and small – indeed, there are new products designed specifically with SMEs in mind.

And basic hygiene responses to these situations are also needed. If systems were locked up, what happens? Do you have business continuity planning, not only to keep a plant running or the lights on, but to call partners, track produce and invoices? Can you maintain food quality when you can't access the software on your computer?

These are the questions we need to ask ourselves. We need to plan for a cyber incident the way we plan for a drought, bushfire or any other natural disaster or financial challenge.

Australian agribusiness must continue to adapt their cyber strategies in line with emerging threats, and it is everyone's responsibility to improve our cyber resilience. This means not only acting as a collective but taking responsibility as individuals to deal with everything from phishing scams to complex cyberattacks.

A culture of cyber alertness and resilience is required, from the board to the factory floor and to the farm gate.

Patrick McClelland
Managing Partner, Porter Novelli Australia and
Deputy Chair, Agribusiness Australia
LinkedIn

David McKeon
Director, Agribusiness Australia
LinkedIn