Fact sheet 1

Cyber security basics for internal and small teams

As agricultural industries' reliance on technology, data and information sharing grows, so does the likelihood of potentially devastating cyber attacks. Cyber security is the responsibility of all employees, and understanding cyber fragility and preparing accordingly will reduce the risk and impact of a cyber attack.

With the increased adoption of technology in agriculture, cyber security is more important than ever. Businesses and organisations with in-house cyber security teams need to understand where their digital vulnerabilities are, be alert to potential threats, and have strategies in place to mitigate their risk.

Implementing a good cyber security team structure is crucial to managing the key essentials of business: risk and cost. Most cyber security-related threats and incidents are brought about by the things people do (or don't do).

Challenges commonly faced

The changing landscape of technology in agricultural businesses brings with it a host of cyber security risks. The added complexity of teams of employees having access to confidential data and information can make organisations even more vulnerable to hackers and security breaches.

Risks include a lack of knowledge, training and awareness of cyber security practices, resulting in ineffective security, key activities such as system updates being performed incorrectly and causing cyber vulnerability, or rapid adoption of new technology without proper consideration of cyber security risks and vulnerabilities.

Agricultural businesses are attractive targets for hackers motivated to steal data for economic advantage or disable systems and demand a ransom for their recovery, and issue-motivated attackers seeking to damage and embarrass businesses in the sector.

What a cyber attack looks like

The most common types of cyber attacks experienced by organisations are:

Phishing scams are emails, text messages or instant messages that appear to come from a trusted individual or institution. They trick the recipient by mimicking wording and branding to appear legitimate, and contain an attachment or link that, when clicked, enable the hacker to gain access to accounts or networks and steal money or sensitive information and data.

Ransomware is a form of malware (malicious software) that encrypts a victim's files and locks down the system. The attacker demands a ransom from the victim to restore access to the data upon payment. Ransomware attacks can happen if a user falls victim to a phishing scam.

Self-motivated insider threat actors target their employer or an entity they have established trusted access to. These actors can cause reputational damage, as well as steal information for profit using their privileged access to do so.

Learn more
agrifutures.com.au/cyber-security-threats

AgriFutures® National Rural Issues

Cyber security for internal and small teams

Fact sheet 1

Protecting your business

Cyber security teams need to work alongside stakeholders at all levels of the business to evaluate risks and mitigation strategies. Cyber security is not just an IT issue – it is everyone's business. By implementing simple cyber security strategies, you can mitigate the risks and reduce the impact of an attack.

- Implement formal HR security processes such as background checks.
- Implement a cyber security training and awareness program.
- Develop a cyber security framework that aligns with international cyber security standards and practices, e.g. ISO 27001, and implement across the organisation.
- When procuring new technology, consider what risks and exposure it may present to the organisation and determine how these will be managed.
- Use a password manager and regularly change default passwords on network-capable devices.
- Conduct regular vulnerability scanning and penetration testing.
- Determine technology configuration requirements during procurement. Consideration should be given to antivirus, encryption, multi-factor authentication and back-up and disaster recovery.

Small businesses are the target of 43% of all cyber crimes. Cyber security threats on farm can include disabling or corrupting 'smart farm' devices, stealing livestock genetic data or accessing sensitive business details.

Secure information sharing

Dealing with suppliers and customers electronically opens several risks, most notably confidentiality and privacy breaches. Think about the information being shared, how it is shared, and who the recipient is.

If sensitive information and data is being shared, use secure file-sharing sites with business-grade security to protect your organisation from being exposed or breaching privacy rules and regulations.

Employees are critical to ensuring effective cyber security. Good hiring practices, strong policies and training programs, access control, and monitoring can greatly reduce the likelihood of an organisation experiencing a cyber attack.

→ Find out more

Read the full report *Cyber security threats – are we prepared? A threat-based assessment of the cyber resilience of the Australian agricultural sector.*

Learn more
agrifutures.com.au/cyber-security-threats

AgriFutures® National Rural Issues