Fact sheet 2

Cyber security basics for third-party management

As agricultural industries' reliance on technology, data and information sharing grows, so does the likelihood of potentially devastating cyber attacks. Failure to manage risks posed by third-party providers can result in potentially harmful consequences.

With the increased adoption of technology in agriculture, cyber security is more important than ever. Outsourcing its management can be a cost-effective way to keep up to date with ever-evolving IT infrastructure, and a dedicated specialist on hand can detect and respond to any issues that may arise.

However, deciding to outsource cyber security management comes with increased risk of exposure to cyber threats. Knowing what to look for and how to choose a reliable service provider will help minimise the impacts on your business in the event of a cyber attack.

Secure information sharing

Dealing with suppliers and customers electronically opens up several risks, most notably confidentiality and privacy breaches. It is important to consider what information and data is 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.

Risks associated with using a third-party provider

Engaging a third-party provider to manage your cyber security means you are trusting them with your data and are reliant on their capabilities, expertise and systems. The risks of this approach are:

Security: The provider falling victim to a cyber attack, in turn exposing its customers and their data.

Operational: Inability of the provider to meet expectations outlined in the contract, causing delays, increased cost and damage to customer reputation.

Access to sensitive information: Access of the provider to sensitive information that if handled incorrectly or maliciously can cause ramifications for the customer.

Integration of new technology: Adoption of new technology without proper consideration of cyber security risks and vulnerabilities.

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

AgriFutures® National Rural Issues

Cyber security basics for third-party management

Fact sheet 2

Key controls

When engaging an external specialist to manage your cyber security, it is important to choose a partner that you trust to look after your most sensitive business information, and clearly define your expectations at the start of your agreement with them.

- Define your cyber security requirements and clearly outline them in your contract.
- Develop a risk assessment procedure that identifies cyber security risks.
- Develop an incident response and business continuity plan.
- Ensure that the contract between your organisation and the service provider covers your basic cyber security requirements, including antivirus, back-up, multi-factor authentication, asset management and incident reporting.
- Maintain an up-to-date list of important software, applications and devices used within your organisation.
- Use a password manager and regularly change default passwords on network-capable devices.
- Define formalised human resource requirements with the provider, including information protection requirements and end-of-employment security reminders.

Threats faced

Third party falls victim to a cyber attack, granting the hacker access to confidential client information.

No necessary data protection laws and regulations in place, resulting in exposure of sensitive information.

An employee or user exploits their privileged access to target sensitive customer or client data in order to cause reputational damage or steal information for personal gain.

Choosing a reputable and trusted provider, having a clear contract or agreement in place that outlines roles and responsibilities, and being aware of cyber threats to your business will increase your cyber security capability.

→ 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