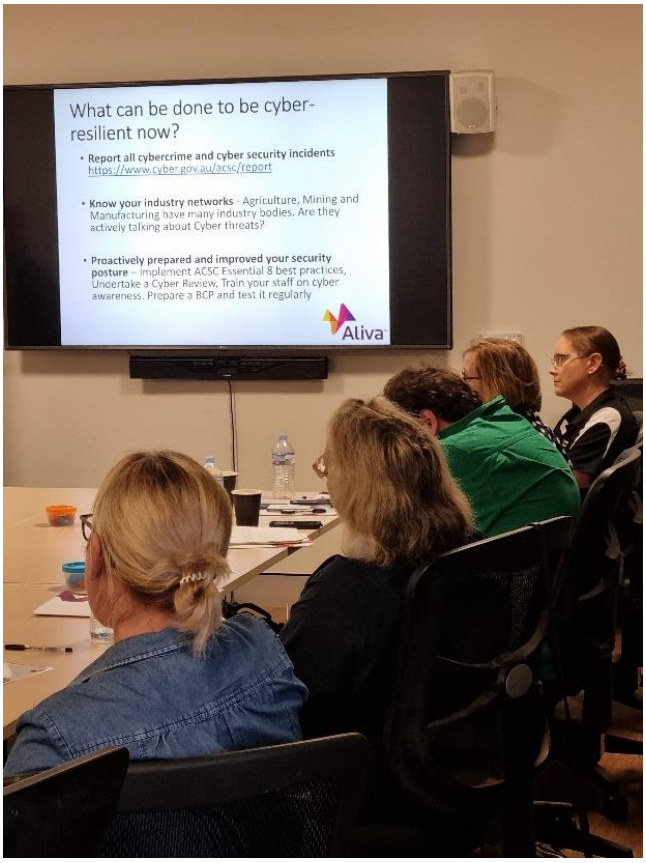
GrazingFutures Livestock Business Resilience Narrative

Cybersecurity in Agriculture – Are the gates locked or left ajar?

Background

Australian livestock producers have adopted the use of technology and digital programs to boost business efficiencies and help meet the demands of the digital world. However, in doing so they are increasingly becoming aware that they have also inadvertently acquired new risks to their businesses. Cyber security is increasingly becoming one of the most important precautions a business needs to act on. However, this is currently a topic poorly understood by most primary producers and small business owners in rural and regional Queensland.

A cyber incident can lead to loss of intellectual property, loss of reputation, finances, as well as the associated losses in time and money associated with finding and fixing the problem. No industry is immune from a cyber-attack.



In March 2023 Aliva, a private Information & Communications Technology solutions provider, presented the Cybersecurity and Your Business Workshops in St George and Roma to provide producers with a greater understanding of cyber security. A key focus of the workshop was to drill down to answering that core question of “Is your Business Cyber Resilient?” by looking at the ways cyber-attackers break into our digital systems.

Glynn from Aliva explained how the threat landscape is constantly changing. New threats emerge, and businesses need to ensure they have security solutions in place to protect against these shifts. Unfortunately, many of us don’t and we often unknowingly put the business at risk of a cyber security breach by not quite closing the metaphoric gate and enabling opportunities for unwanted intruders.

Australian Government | Future Drought Fund | Drought and Climate Adaptation Program | Queensland Government

This program is jointly funded through the Australian Government’s Future Drought Fund and the Queensland Government’s Drought and Climate Adaptation Program.

The workshop covered off on why business owners and individuals need to be cyber aware and what happens if they are attacked. Awareness of cyber security was considered to be one of the greatest tools in preventing attacks. Aliva also focused on terminology, what businesses can do to mitigate against cyber-attacks, and the importance of a Business Continuity and Disaster Recovery Plan.

All participants in the workshops found it highly valuable and had identified areas for immediate improvement in their businesses to ensure they were cyber secure.

Is your Business Cyber Resilient?

When participants were asked to explain any planned changes, they would make to ensure cyber resilience of the business, there were four main areas identified: backing up, passwords & password management, anti-virus protections and increased cyber security awareness across their team.

Awareness

Cyber security awareness is one of the most important mitigation practices for protecting a business against sophisticated attacks and scams. Being cyber security aware means, you are essentially creating a 'human firewall' against cyber-attacks.
It's critical for a business owner to understand what their information assets are, where and how they are accessed by staff, advisors, contractors, and in the case of businesses run from the home, visitors.
Everyone involved in accessing the hard drive, documents, servers, online cloud drives and Wi-Fi shared by the business should be trained to be aware of potential security threats and what steps need to be taken to protect the businesses information and technology assets.

Several participants stated they will educate employees and family about cybersecurity. Participants were also interested to learn the legalities preventing ransoms being paid when businesses are held ransom via a ransomware attack.

Backups

Most businesses understand the importance of backing up data to avoid the negative impact of data loss on their operations. Backing up and having backups mean you can restore your files if something goes wrong. It is a precautionary measure so that your data is accessible in case something happens to your computer. Aliva recommended backing up these important files regularly to an external storage device and offsite on an online server such as the cloud.

Setting up a system to automatically back up all important documents regularly is also recommended.

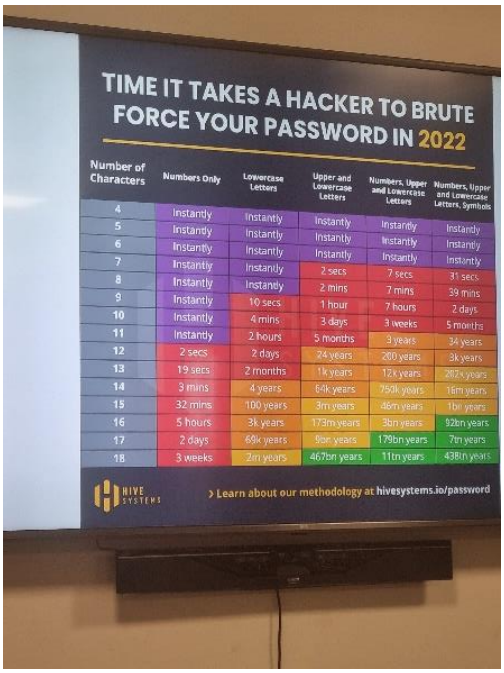
A single copy of critical data may seem to be sufficient to recover from, however, at the heart of every robust data protection plan is the 3-2-1 backup rule. This is a universally accepted strategy within the IT industry, referring to a tried-and-tested approach to data retention and storage. The 3-2-1 backup rule refers to:

3. Keep at least three (3) copies of data.
2. Store two (2) backup copies on different storage media.
1. Store one (1) backup copy offsite.

By applying this rule, you ensure that data can be recovered in almost any failure scenario. One of the most common practices is to keep one copy of production data, one backup on a local repository and one backup copy in offsite storage or in the cloud.

Password & Password Management

In today's digital world, business is generally bound using passwords and usernames to verify the identity of a user during the authentication process. But the importance of ensuring a password is strong grabbed many people's attention as Glynn showed a chart showing the estimated time it would take to crack passwords of different lengths and characters using a brute force attack. The chart revealed that all passwords of 7 and less characters can be cracked in a maximum of six minutes. It also showed passwords of 10 characters consisting exclusively of numbers can be cracked pretty much instantly. To be secure, a high number of characters consisting of a combination of numbers, upper and lowercase letters, and symbols must be used.



Participants were interested in learning about safe password managers and adopt the use of these systems, as well as multi-factor authentication.
Password managers are a great way to keep business passwords safe and secure – as they keep usernames, passwords, and associated websites in a secure digital vault. There are many options for password managers, and most anti-virus software providers also offer password managers.

Multi-factor Authentication (MFA) is an authentication method that builds an extra wall of security above passwords by requiring the user to provide two or more verification factors to gain access. MFA requires one or more additional verification factors beyond a username and password. There is a belief amongst the ICT specialists that MFA will scale down the need for passwords in the future.

Antivirus protections

The presence of viruses and other malware on the internet is constant and always changing. Hackers are constantly developing new forms of software, most going undetected by the user.
Antivirus protections scan the computer, tablet or smartphone for viruses and help remove malware files that may have entered. They can also identify online threats and cause hidden threats to reveal themselves.

Several participants said they would check the current antivirus protections they had in place, and one wanted to add antivirus protection to the mobile phones attached to the business.

You Must Have a "Business Continuity Plan"

Having a documented Business Continuity Plan for computer systems is defining how the business will operate if access to technology and information for an indefinite period. It is

becoming more critical to consider how to be proactively prepared and have a planned response outlined. Time is critical when a business is disabled by malware or viruses, so adding a business continuity plan to an overall business resilience plan means having an immediate path of action and reduce business losses.

The Essential Eight

The Australian Cyber Security Centre (ACSC) has developed prioritised mitigation strategies to help organisations protect themselves against various cyber threats. The most effective of these mitigation strategies are the Essential Eight. The Essential Eight are core mitigation strategies to avoid succumbing to a cyber incident or attack. According to the ASD, the Essential Eight are effective in protecting against around 85 per cent of targeted cyber-attacks.

1. Application Whitelisting To control the execution of unauthorised software.	**5. Restrict Admin Privileges** To limit powerful access to systems.
2. Patching Applications To remediate known security vulnerabilities	**6. Patching Operating Systems** To remediate known security vulnerabilities.
3. Configure Macros To block untrusted macros.	**7. Multi-Factor Authentication** To protect against unauthorised access.
4. Application Hardening To protect against vulnerable functionality.	**8. Daily Backup** To maintain the availability of critical data.

Wrap up - The value of the workshop to grazing businesses

Prevention is key, and Glynn from Aliva recommends all small businesses have a Business Continuity and Disaster Recovery Plan in place. If the worst case is realised, having a plan will map out how your business will continue to operate, if possible.
The threat landscape is constantly changing. New threats emerge, and businesses needs to ensure they have security solutions in place to protect against these shifts.
Become cyber security aware.

Glynn also recommended a visit to the suite of StaySafeOnline1 videos available for free on YouTube - https://www.youtube.com/user/StaySafeOnline1.
StaySafeOnline1 is the official YouTube channel of the National Cyber Security Alliance, which aims to educate and empower a digital society to use the Internet safely and securely at home, work, and school, protecting the technology individuals use, the networks they connect to, and our shared digital assets.

The Australian Cyber Security Centre (ACSC) has developed prioritised mitigation strategies to help organisations protect themselves against various cyber threats. The most effective of these mitigation strategies are the Essential Eight. The Essential Eight are core mitigation strategies to avoid succumbing to a cyber incident or attack. According to the ASD, the Essential Eight are effective in protecting against around 85 per cent of targeted cyber-attacks. More information from ACSC can be found via www.cyber.gov.au

Prepared by Gina Mace and Rhonda Toms-Morgan, ConnectAg. rhonda@connectag.com.au