Hacking a wake-up call for agribusiness
By ANDREW MARSHALL

Farm Weekly
Thursday 17th November 2022
821 words
Page 28,29 | Section: FARM
414cm on the page

Hacking a wake-up call for agribusiness

By **ANDREW MARSHALL**

SMALL to mid- sized businesses might be the backbone of the Australian economy, but they are also unprepared and under-resourced for the rapidly rising challenges of a digital world.

While headlines about cyber security breaches at big name outfits including Medibank Private, Optus and international meat processor JBS, have provoked public alarm about personal data falling into criminal hands, more modest family businesses and mid-sized companies are just as vulnerable.

"Many cyber attacks are not performed by sophisticated hackers," said Scott de Mestre, the head of security at employment relations and work health and safety firm, Employsure.

"They are executed by people with the basic knowledge of how lax businesses can be."

Australian businesses of all sizes were increasingly lucrative targets for cyber criminals as they launched more attacks, with increasing severity, potentially exposing a business' supply chain customers, too.

Every eight minutes the Australian Cyber Security Centre averages a call reporting a data hack or security breach issue.

"There is a glaring lack of knowledge in small to medium sized businesses when it comes to cybersecurity," Mr de Mestre said.

Busy farm sector enterprises were potentially more vulnerable than many as their owners juggled a multitude of roles, had limited information technology skills and dealt with many internet-based transactions and correspondence.

The total economic impact of cybercrime was put at $3.5 billion in Australia in 2019, while in 2021 payment redirection scams alone jumped 77pc on the prior year to cost businesses almost $230m.

"Scamwatch data showed small and micro businesses lost the most money to scams last year," said Australian Competition and Consumer Commission deputy chairman, Mick Keogh.

"Farm businesses lost over $1.5m to scammers impersonating a business or its employees with convincing emails requesting an upcoming payment be redirected to a fraudulent bank account.

"The most common scams targeting farmers involved the sale of tractors and other farm machinery, with losses of $1.4m reported in 2021."

At the same time, one in three Australian consumer households may have had their personal information stolen by criminals, according to information security advisory group ISACA.

"The data breaches we now hear about really put into context the fact that anybody is vulnerable," said Agribusiness Australia director and former GrainGrowers Limited chief executive officer David McKeon.

"It's a reminder of the significance of some of these threats, regardless of the size of your business."

He said while larger agribusinesses could fall back on sophisticated IT security systems and implement simulated action plans to prepare for hacking attacks, farm sector enterprises of all sizes must promote a culture of alertness to potential risks.

Most agribusinesses, however, were fortunate in being less likely to be targets of high profile ransomware hacks by sophisticated criminal operations, according to chief executive officer at corporate public relations firm Porter Novelli, Rhys Ryan.

"Most agricultural companies

and food processors are not juicy targets who handle lots of sensitive information, but it's quite possible that hackers still regularly get into their networks and check them out," Mr Ryan said.

His firm was frequently involved in preparing companies with preventative strategies and a plan of action they need to take in the event of a cyber security crisis occurring.

Aside from the costly multi-million dollar blackmail payments they would demand, cyber hackers breaking into a food processing sector supply chain or marketing network could create massive disruption and reputational damage to an agribusiness, its customers and suppliers if the criminals locked or encrypted a target's files.

"A lot of other costs are involved, too – forensic IT specialists, legal fees, communications specialists to deal with customers, lost revenue, the list goes on," Mr Ryan said

Even the most basic attempts to extract money from companies via phishing emails could be very costly if any business was not alert to the risks.

Mr McKeon said one of the biggest cyber security risks for business was their own staff.

"Training yourself and any employees to know what to be aware of, and having regular conversations with your bank or IT professionals, would be obvious starting points to improve resilience to a cyber hacking threat," he said.

Clicking on random invoice emails, which were in fact, fakes, or using public Wi-Fi to access the business network were the sort of mistakes everybody needed to learn to avoid.

Mr de Meste said small business owners could not afford to ignore cyber security.

He said they needed a basic understanding of what it entailed, how strong their systems were, and what policies or procedures need to be in place.

Mr de Meste noted the Australian Cyber Security Centre's website contained a helpful wealth of valuable information tailored for small and medium businesses which should assist with the basics.

However, some things were best left to the experts and therefore delegating some tasks to trained cybersecurity specialists could be a more efficient way to protect the business.