Waterstons
we're with you

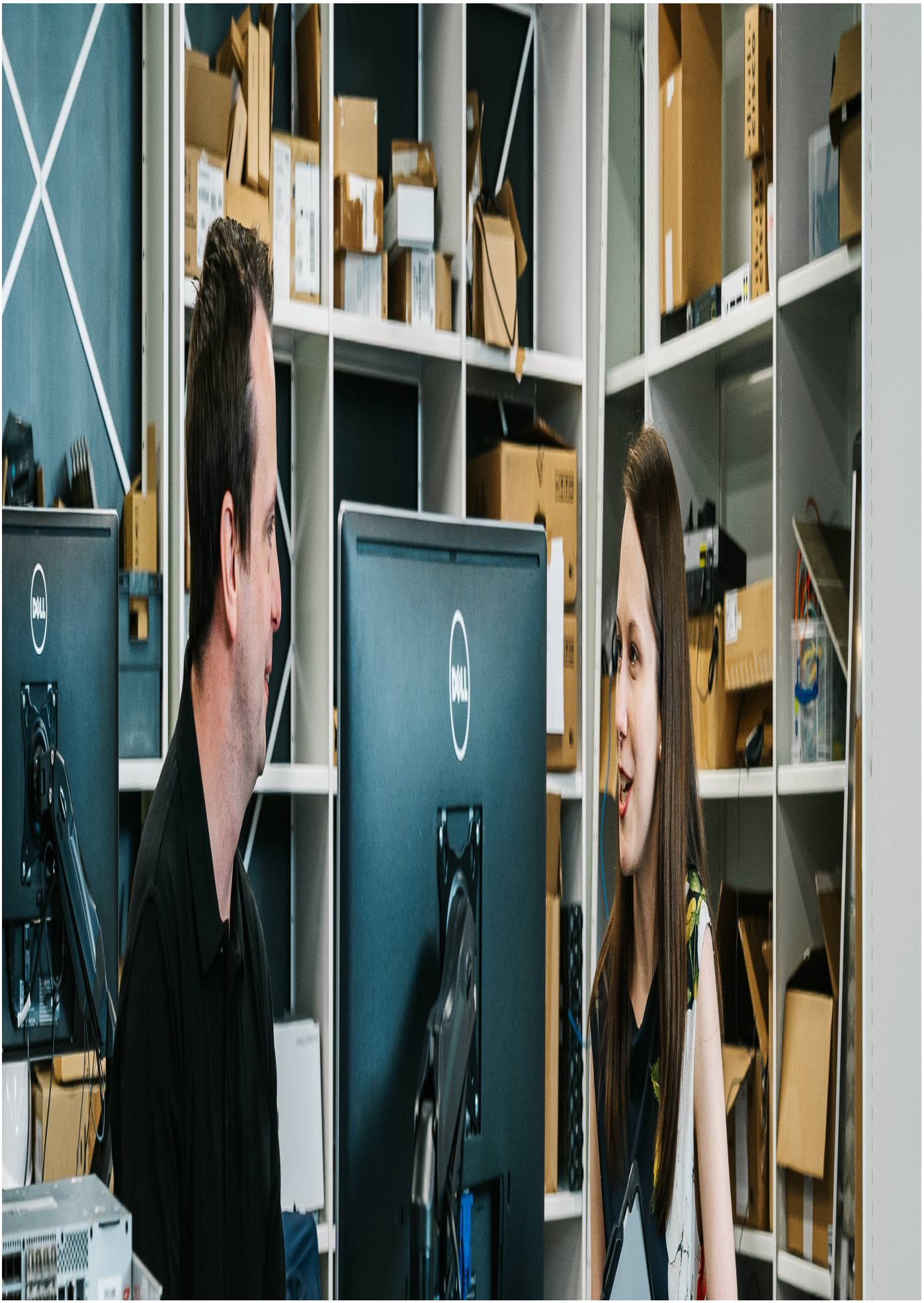
+44 345 094 0945
www.waterstons.com

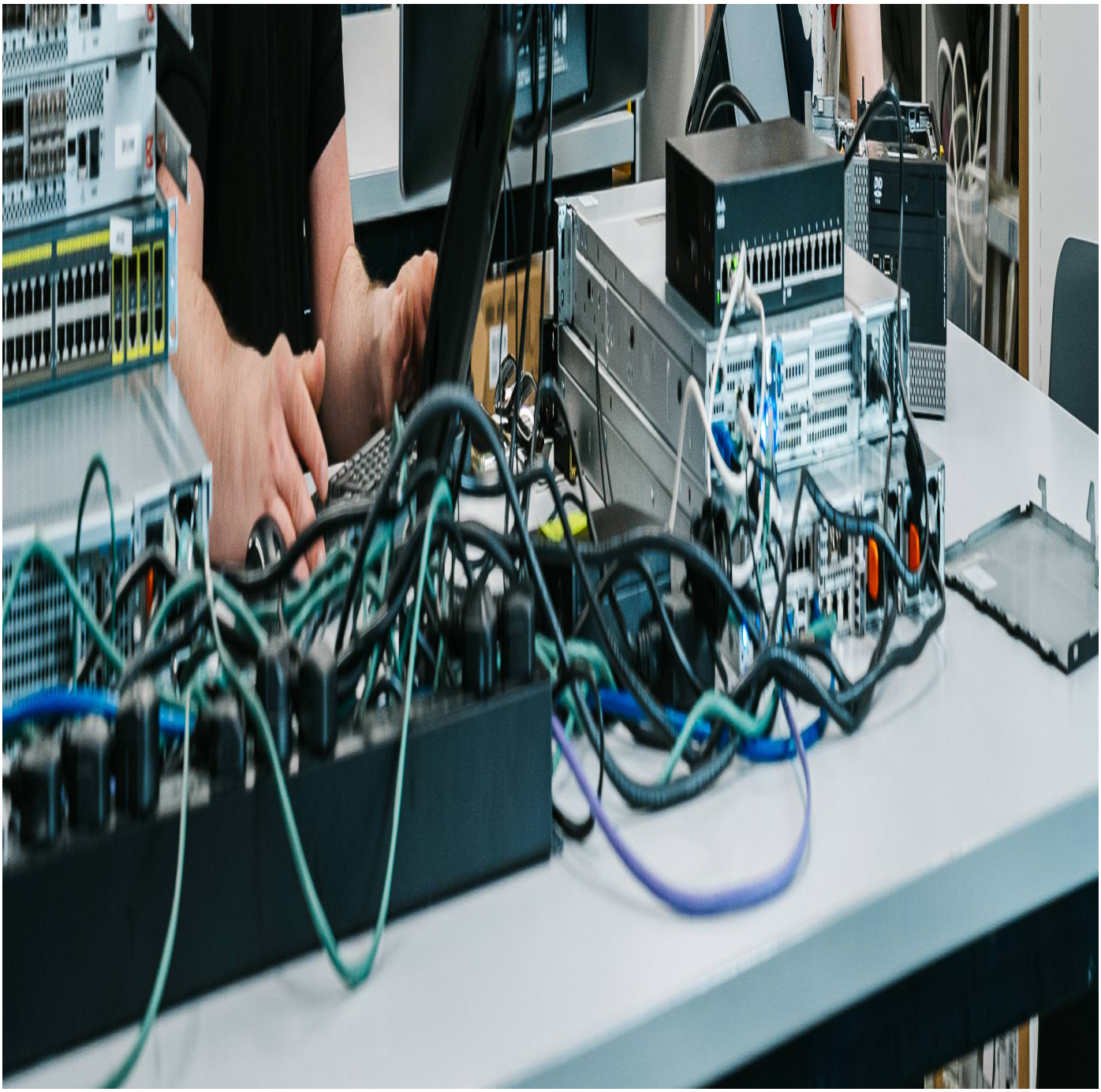
Article

Jun 2023

Beyond the Ransom: The Collateral Damage of Cyber Attacks on Primary Food Production

Picture a typical food production enterprise: a complex web of interconnected processes and systems, all of which are increasingly digitalized and automated. Then imagine the chaos if a ransomware attack were to suddenly shut down those systems. Immediate production disruption is the first domino to fall, leading to downtime, loss of perishable goods, and financial distress.





When a primary food production enterprise falls victim to a cyber-attack the effects reverberate far beyond the compromised computer systems of the targeted company. The consequences are akin to ripples spreading across a pond, extending to the wider food supply chain, the consumer, and potentially the entire food economy.

Picture a typical food production enterprise: a complex web of interconnected processes and systems, all of which are increasingly digitalized and automated. Then imagine the chaos if a ransomware attack were to suddenly shut down those systems. Immediate production disruption is the first domino to fall, leading to downtime, loss of perishable goods, and financial distress.

In a striking illustration of the real-world consequences of cybersecurity threats in the food production industry, we can look at the unfortunate events that unfolded in 2021. Global meat processing giant JBS Foods fell victim to a ransomware attack that had far-reaching ramifications. This attack, *as reported by ABC News,* not only resulted in JBS Foods paying a staggering $14 million ransom, but it also brought production to a grinding halt both domestically and internationally for five agonizing days.

The ripples then spread to the supply chain. A cog in the machine that is the food production system comes to a grinding halt, and the entire mechanism stutters. Retailers face product shortages, raising the spectre of increased prices and frustrated customers. Other enterprises within the chain also feel the burn. They might depend on the compromised company for a key ingredient or component, and without it, their own production suffers.

Next, we come to the consumer, whose trust in the company, and possibly the wider industry, can be undermined when breaches compromise their data. The consequences could become even more grave if the quality control systems are targeted, resulting in safety issues or contaminated products. The damage to the company's reputation and consumer trust can be a long-lasting scar, far outliving the immediate incident.

Then there's the inevitable financial fallout. The direct costs of cyber-attacks – remediation expenses, potential ransom payments, and loss of revenue due to disruption – can be crippling. Yet, the financial haemorrhage doesn't stop there. Indirect costs such as higher insurance premiums, expenses for improving cybersecurity measures, and potential legal penalties for negligence add to the toll.

Regulators, too, are quick to respond to such incidents. A company exposed to cyber-attacks due to lax cybersecurity measures could face severe penalties, doubly so now if your enterprise is considered critical infrastructure. Moreover, major incidents often spur regulatory bodies into action, bringing about tighter regulations for the entire industry in a bid to avert future attacks. When it comes to food production though there is more than one regulator to consider.

Regulatory bodies, such as the Australian Department of Agriculture, Water and the Environment, and the Food Standards Australia New Zealand (FSANZ), have acknowledged the need to address cybersecurity concerns within the food production industry. They have issued guidelines, standards, and requirements that food companies must adhere to, to protect their digital infrastructure and ensure the integrity of their operations.

One significant regulation in Australia is the Food Standards Code. This Code sets out specific requirements for food safety and quality. Recognizing the growing threat landscape, the Code now encompasses cybersecurity as a critical consideration. Food companies are expected to implement robust cybersecurity measures to prevent unauthorized access, tampering with critical processes, or compromising sensitive data related to food production.

To enhance cybersecurity resilience, companies are encouraged to follow industry best practices and frameworks. The Australian Signals Directorate's Essential Eight and the Australian Cyber Security Centre's guidelines provide valuable recommendations for organizations to strengthen their cybersecurity posture. These frameworks emphasize risk assessments, regular monitoring, incident response planning, and employee awareness training as crucial elements for maintaining cybersecurity readiness.

Cybersecurity in the primary food production industry is not just about protecting a single enterprise, but about safeguarding an interconnected ecosystem that stretches from the farm to the dinner table. It's a call to action for food production enterprises to fortify their digital defences with robust cybersecurity measures, including regular system updates, rigorous access controls, comprehensive employee training, and well-planned incident response strategies. Collaborating with cybersecurity experts for regular system audits can also help identify and patch potential vulnerabilities, bolstering the resilience of our food production systems.

If your enterprise needs assistance or advice navigating this complex and ever-changing environment, reach out to Waterstons. We're with you.