FOOD & GROCERY

Sector Overview

If an 'Army marches on its stomach', or so the saying goes... what does a nation need to keep moving? The answer surely is a fully functioning agri-industrial food and grocery sector held together by a web of logistics.

The Food & Grocery sector is large, complex, and not easily compartmentalised in a neat box. The SOCI legislation definition of a critical food and grocery asset was limited to the network that supplies or distributes essential food and groceries. Yet, there was no prescriptive or detailed list of what food and grocery infrastructure actually is in the legislation when it comes to what is considered 'essential' on the basis that this 'may evolve over time.'

Food security supply chains were under stress during the global pandemic and this external shock provided 'food for thought' (pun intended) on how cyber-attack might impact the food and grocery sector. The systemic stress of the pandemic is why the sector gained an extension of time (until 1 January 2023) to meet SOCI compliance standards regarding risk management program obligations. Through the government's SOCI consultation process, food and grocery industry perspectives claimed that essential groceries were considered by some to include fruit and vegetables, grains, dairy products, eggs, oils, tinned and dried produce, meat, fish, toiletries and over-the-counter health products.

It is obvious to everyday Australians that there is concentration risk in the food and grocery sector with two major supermarket chain stores each having roughly a thirty per cent share of the grocery retail market, the value of which surpasses $100 billion Australian dollars annually. COVID-19 reduced in-store buying and led to significant growth in online retail spending on groceries and alcohol. A 2021 survey revealed that more Australians than ever before preferred to shop for food online, thus increasing the cyber threats to digital channels.

Beyond the digital transformation of retail food and grocery, the agriculture, fisheries, and forestry sectors that support food and grocery have also experienced rapid digital transformation, that in turn increased the cyber-attack surface of the sector.

Factors contributing to increased food & grocery sector cyber threats:

The Covid-19 pandemic created an array of new challenges for the sector. Employee turnover and labour shortages increase the risks of human error and security awareness as new staff are trained up. Already constrained supply chains can result in increased pressure to pay ransoms in order to avoid missing shipments following a successful ransomware attack.

In Q1 2022, one of the most common reported intrusion techniques used against the retail industry victims was social engineering, especially conversation hijacking. This technique is intended to make it harder for victims to detect malicious behaviour and uses vectors such as phishing emails, text messaging, and voice calls. Social engineering will almost certainly remain a threat to the food & grocery sector as malicious campaigns are relatively effective, offer a high return on investment, and can cause significant damage.

Legacy systems

Much of the industrial technology used in the food & grocery sector is older operational technology where security protocols and basic cyber hygiene are likely to be non-existent. Legacy systems that are internet-connected are less likely to have the necessary security updates installed. Cyber-attackers are aware of this and actively scan for older systems to use as entry points into a company's technology infrastructure. Regardless of the size of the business, it's vital for organizations to understand the risks associated with not adequately segregating legacy industrial assets and their newer corporate technology networks. The food and grocery sector is in a period of digitalisation, adopting more remote controls and a remote workforce.

Food & Grocery Sector Attacks:

2020 and 2021 saw a spate of food and grocery sector attacks:

- A cyberattack on American JBS Foods (the largest meat processor in the world) led to the suspense of operations at its global beef processing plants. JBS paid the attacker, ransomware group REvil $11 million US dollars in Bitcoin so that it could recommence operations. JBS paid the ransom to lessen the impact on its supply chain partners, such as eateries, supermarkets, wholesalers, and ranches. This attack had a direct impact on Australia as operations were suspended at 47 sites around the country due to systems for meat processing and quality assurance being locked down as a result of the attack.
- One of Australia's largest breweries, Lion, was threatened with a $1 million ransom demand to prevent the publication of its private data on the dark web. The attack caused a partial outage to Lion systems.
- Major food logistics company Toll Group had its IT systems shut down twice in the space of three months as a result of ransomware attacks. Toll Group is a multinational logistics provider that provides freight, storage, and distribution services.

Evaluation:

Ransomware is the most common attack type used to target the food and grocery sector, with most attacks in the sector undertaken by Russian-speaking threat actors. Since February 2022, when the Russian war in Ukraine began, cyber-attacks by Russian-speaking threat actors have targeted farmers at the peak of the harvest season with a belief that rising food prices and shortages will force a speedy ransom payment. Russian-speaking threat actors have also been observed targeting online Western food and grocery retailers operating in emerging economies.

Agriculture Link to Food & Grocery Sector Cyber Threats:

The agricultural sector in Australia was ranked sixth most likely to suffer a data breach in 2019, with ransomware, phishing, scam emails, and malware all represented leading threat vectors. The now-defunct Russian-speaking REvil ransomware group had explicitly vowed to keep attacking the agricultural sector and its supply lines.

Both small and large Australian agricultural businesses suffer from a lack of cybersecurity maturity despite significant investment in digitalisation across the sector. Cybercriminals see the sector as a rich target for acquiring financial and personal data through payment gateways and computerized agricultural equipment. Agricultural business data, production systems, intellectual property, drones, robotics, autonomous vehicles, and remote sensing technology are also at risk.

The nation's food supply chain is made up of several interdependent businesses. A halt or slowdown during harvest season, for instance, might have an impact on the entire industry as food distribution networks and processing facilities experience the consequences of possible events that may have occurred weeks or months earlier. Restaurants and retail establishments require a dependable and accessible supplier of food supplies. Any disruption from a cyber-attack may lead to price increases or shortages that have an impact on people's daily lives.

Responding to threats against the energy sector in Australia:

Most food and grocery sector entities won't be able to share 'machine to machine' intelligence, so an industry partner is needed as the enabler/facilitator for cyber threat intelligence (CTI) and collective defence via other means. By taking on the role of the trusted advisor/facilitator for the intelligence exchange, an industry organisation would ensure the overall quality of information flowing through its systems and out to the CI members.

'Forewarned is Forearmed', and by joining a trusted cyber community of Critical Infrastructure owners and operators responsible for protecting their food and grocery infrastructure assets, you can join the movement to share contextual intelligence and proactively approach cyber defence. Cyber threat activity shared into the CI-ISAC ecosystem by one member has the potential to help others across the sector and the broader CI community stop similar attacks before they impact operations.

CI-ISAC, as a not-for-profit, member driven organisation, with a mission to serve its members and in turn their customers by building a trusted community and leveraging the best technology in its intelligence platform, and drawing on resources and resilience through its industry peer-to-peer network to anticipate, mitigate, and respond to cyber threats.

More information on CI-ISACs sovereign intelligence-sharing capability can be found on the official website: https://www.ci-isac.com.au , or by emailing info@ci-isac.com.au.

Published: 17th February 2023