FRESH PRODUCE SAFETY CENTRE
AUSTRALIA & NEW ZEALAND

FOUNDING PARTNERS
THE UNIVERSITY OF SYDNEY
pma AUSTRALIA+NEW ZEALAND

FACTSHEET – FOOD DEFENCE FOR THE FRESH PRODUCE INDUSTRY

December 2021

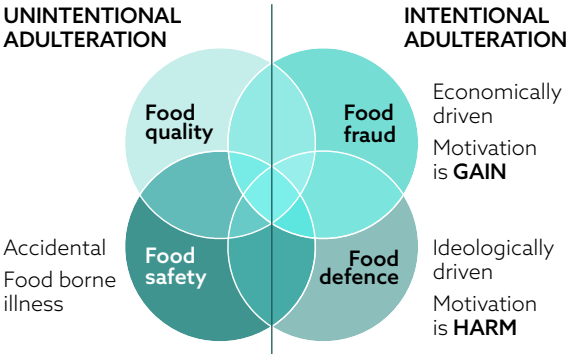
Written by Dr Kim-Yen Phan-Thien
Sydney Institute of Agriculture, Faculty of Science, The University of Sydney, NSW 2006, Australia

This fact sheet contains concise background information and practical advice on food defence in the fresh produce industry. It aims to help growers, packers, and processors in Australia and New Zealand determine a relevant approach to food defence for their business.

1 Background

1.1 How is food defence different to food safety?
The risk assessment and management of food defence threats are quite different to that of food safety hazards. Food defence is about protecting the food supply from malicious attack, especially where this could lead to unsafe products that

Figure 1. Types of food risk (GFSI, 2018)



cause public harm, whereas food safety is about protecting food from unintentional (accidental or naturally occurring) contamination.

Food safety risks can be assessed and managed on a scientific basis. For example, microbiology and biochemistry help us to understand the persistence of pathogenic bacteria and pesticide residues on produce. In contrast, threats of malicious attack are much more difficult to predict. An attacker may select from a large range of potentially hazardous biological, chemical, physical, or even radiological agents to tamper with food, and they may introduce the contaminant to the supply chain in unexpected ways.

The business impacts of a malicious attack, incident response, and authority leading an official response, also differ to that of a food safety incident. For example, outbreaks of foodborne disease are governed by food safety laws, and investigations are coordinated by relevant food and health authorities. However, an outbreak caused by intentional contamination (i.e., food tampering) would be governed by criminal laws and involve a police investigation, alongside necessary food safety and public health responses.

1.2 What types of threat does food defence address?

Malicious (intentional) contamination is a particular concern for industry and governments because such incidents can compromise the safety of food and place public health at risk. However, food defence can be applied to a range of threats (Table 1), each of which has potential to harm your business, directly or indirectly.

1.3 Who carries out these threats?

Perpetrators of malicious attack are motivated by personal or ideological drivers (Table 2). These motivations influence the goals, methods, and intended outcomes of their attack. Attackers who deliberately contaminate food do so with a criminal intent to cause harm, fear, or dread. To this end, they may use methods that cause widescale illness, death, and disruption.

1.4 Why is food defence relevant for my business?

Food defence is relevant for food businesses at all stages of the supply chain – including growing, packing, and processing of fresh produce. We are

Table 1. Types of threat (PAS 96:2017)

Type of threat	Examples
Economically motivated adulteration	• Substitution with a cheaper ingredient • Adulteration to 'extend' a more expensive ingredient (e.g., in processed products that contain secondary ingredients)
Malicious contamination	• Intentional introduction of a contaminant to food • Intentional introduction of an allergen to food or to the processing facilities
Extortion	• Threat of attack unless demands are met
Espionage	• Theft of intellectual property (e.g., proprietary plant varieties, innovative/patented technology) • Theft of confidential information (e.g., customer data, sensitive business data)
Counterfeiting	• Fraudulently passing off an inferior product as an established, reputable brand
Cybercrime	• Hacking of internet payment system • Hacking of computer information system for industrial espionage • Identity theft for procurement fraud

particularly concerned about the possibility of food being deliberately contaminated, as this can lead to illnesses and deaths. An incident also causes severe financial costs, business disruption, and loss of consumer confidence. Malicious contamination of food is rare, but the threat of attack is real. Recent examples in Australia and New Zealand include:

- **Strawberry tampering.** Sewing needles were deliberately inserted in strawberries produced in Queensland in September 2018. The event rapidly escalated with 'copycat' tampering of strawberries and other produce across multiple states and territories in Australia, and in New Zealand. By the end of the crisis, 230 incidents were reported in Australia, with 68 brands affected, significant financial losses, and negative impacts on export volumes. A former employee was accused of the initial offences, but charges were later dropped.

- **1080 blackmail threat.** Letters containing infant milk formula mixed with 1080 pesticide were sent to the CEOs of Fonterra and Federated Farmers in November 2014. The letters conveyed a threat to contaminate such formulas, and thus damage key export markets, unless the New Zealand government stopped using 1080 for pest control. A businessman with stakes in an alternative pesticide was eventually charged with the crime. The direct cost of the incident to the New Zealand economy was estimated at more than $37 million.

Table 2. Perpetrators of malicious attack

Type of perpetrator	Motivation	Example goals
Extortionist	Personal gain	• Intimidate the victim into meeting their demands (e.g., for money, assets, influence, or impact)
Irrational or disgruntled individual	Personal issue	• Take revenge on (former) co-workers, supervisor, or employer • Endanger an estranged spouse's livelihood or cause them problems • Sabotage or disadvantage a competitor • Gain notoriety or feel powerful • Alleviate boredom (act randomly)
Extremist or Terrorist	Ideological views	• Damage a business/industry to which the perpetrator is opposed • Increase media attention and awareness for an issue • Intimidate a government or community into meeting their demands

1.5 Key terms and definitions

Term	Definition
Contaminant	• Any biological or chemical agent, foreign matter, or other substances that may compromise food safety or suitability. (FSANZ)
Food defence	• The process to ensure the security of food, food ingredients, feed or food packaging from all forms of intentional malicious attack including ideologically motivated attack leading to contamination or unsafe product. (GFSI)
Food fraud	• A collective term encompassing the deliberate and intentional substitution, addition, tampering or misrepresentation of food, food ingredients, feed, food packaging or labelling, product information or false or misleading statements made about a product for economic gain that could impact consumer health. (GFSI)
Food safety	• Assurance that any product within the GFSI scopes of recognition (e.g. food, packaging, feed, etc.) will not cause an adverse health effect for the consumer when it is prepared and/or consumed and/or used according to its intended use. Umbrella term to define any product which is subject to GFSI scope of recognition. (GFSI)

Aside from mitigating the risks of attack, food defence is increasingly important as a prerequisite to supply the retail markets. The latest Global Food Safety Initiative (GFSI) Benchmarking Requirements include a food defence plan alongside a HACCP plan, GMPs, food fraud vulnerability assessment, and supplier management program. Food defence is thus a requirement of GFSI-benchmarked certification schemes such as Freshcare FSQ, BRC Global, FSSC 22000 and SQF.

2 What are the general principles of food defence?

2.1 Food defence plan

The approach to food defence favoured by the Australian food industry is the Threat Analysis Critical Control Points (TACCP) framework set out in standard PAS 96:2017. This framework can be applied to any business in the food supply chain and covers a broad range of threats including malicious adulteration, espionage, cybercrime, economically motivated adulteration, extortion, and counterfeiting (Table 1). The four main components of TACCP are risk assessment, critical controls (i.e., risk reduction and mitigation), incident response, and review/update (Figure 2).

Businesses that export produce to the USA also need to be aware of their obligations under the Food Safety Modernization Act (FSMA). The FSMA food defence rules are focused on intentional adulteration that are intended to cause widescale harm (e.g., an act of terrorism). FSMA requires a food defence plan based on Hazard Analysis and Risk-Based Preventive Controls (HARPC). HARPC combines HACCP and TACCP approaches, in that the hazards encompass both food safety and food defence threats, and the controls include preventive controls and mitigation strategies that are not necessarily critical control points. The FDA website on food defence provides a range of free tools and resources that businesses may find helpful, such as a plan builder tool, mitigation strategies database, and employee training module.

Figure 2. TACCP-based framework for food defence (PAS 96: 2017)

Table 3. Threat assessment – example questions (PAS 96:2017)

Target	Consider your business and ask yourself...
Product	• Is your product used as an ingredient in a wide range of popular foods? • Have there been unexpected increases or decreases in demand?
Premises	• Are hazardous materials, which could be valuable to hostile groups, stored on site? • Do any employees have reason to feel disgruntled or show signs of dissatisfaction?
Organisation	• Do you have a celebrity or high profile chief executive or proprietor? • Do you or your customers supply high profile customers or events?
Information systems	• Do you use Supervisory Control and Data Acquisition (SCADA) and other control systems (e.g., for process, irrigation, and glasshouse automation) that are also used by other organisations, which could be prime targets?

2.2 Threat assessment

The first stage of TACCP is threat assessment to identify threats that are relevant to your specific business, and to prioritise these according to risk, i.e., the likelihood and severity of an incident.

Standard PAS 96 poses a series of questions to help you evaluate the risks of your product, premises, organisation, and information systems being a target of attack. The questions are quite general as they are designed to encompass a diverse range of threats (Table 3).

CARVER+Shock is the framework favoured in the US for vulnerability assessment. It is a military prioritisation tool that evaluates the attractiveness of a target for attack according to seven attributes (Table 4). CARVER+Shock has been used for **sector-wide vulnerability assessment** but can also be applied to assess threats to points/areas within your business. The FDA has **rubrics and worksheets** for scoring each attribute, but you could also use the framework simply to guide discussion/reflection on your supply chain vulnerabilities.

Table 4. CARVER+Shock framework for vulnerability assessment

Attribute	Description	For different points/areas of your supply chain, ask yourself...
Criticality	Measure of public health and economic impacts of an attack	• How many deaths and illnesses could an attack cause? • How much economic harm could an attack cause?
Accessibility	Ability to physically access and egress from target	• How easily could an attacker access your facilities? • How long are their activities likely to remain unobserved?
Recuperability	Ability of system to recover from an attack	• How long would it take your business to recover productivity? • How long would it take for customer demand to recover?
Vulnerability	Ease of accomplishing attack	• How easily could an attacker introduce sufficient contaminant to your product, such that it would be sufficiently distributed, to achieve their aims?
Effect	Amount of direct loss from an attack as measured by loss in production	• How much loss in production could an attack cause?
Recognisability	Ease of identifying target	• How recognisable is the target? E.g., could someone untrained recognise it, or would you need to be an expert?
Shock	Combined health, economic, and psychological impacts of an attack	• How much symbolic importance does the target have? • How much shock value does it have? E.g., would it cause mass casualties, harm children or the elderly?

2.3 Critical controls
Even though the threat of malicious attack is unpredictable, it is still possible to implement control measures. It may be helpful to consider controls in terms of preventive and mitigation strategies.

Preventive strategies reduce the risk of an attack from occurring in the first place, essentially by limiting the ability of an attacker to access their target. The nature of preventive barriers depends on the threat context. For example, physical/ electronic security systems help to prevent unauthorised intruders onto your site. Secure recruitment policies and pre-employment checks help to prevent dangerous individuals from entering your workforce. A firewall helps to prevent an attack on your computer network.

Mitigation strategies reduce the impacts of an attack if it does take place. Systems for monitoring and detecting threats are an important element of this, as the earlier an attack is detected, the more opportunity there is to respond and minimise the harm it causes.

2.4 Incident response
The purpose of food defence is to reduce the risk of malicious attack, but it is not possible to eliminate threat entirely. It is important to plan how you will respond if an attack does take place, to minimise the impacts of an incident and help your business to recover as quickly as possible. Some aspects of a response plan include:

- Damage control – actions to minimise physical and financial harm.
- Collaboration with authorities, e.g., police, food and health authority, industry bodies.
- Business continuity – how to maintain essential business functions and adapt to non-routine conditions.
- Crisis communication – including stakeholder and public communications.
- Restoration of consumer confidence.

Standards for business continuity management (e.g., AS/NZS 5050:2020 or ISO 22301:2019/ISO 22313:2020) may be useful when planning incident response. These focus on organisational resilience to disruptions, where a disruption is any unexpected change in the business environment, or an unanticipated consequence of a planned change, that cannot be managed by business-as-usual. This includes anything from a change in customer requirements, new competitor, or emerging technology, to a natural disaster – but can also be applied to malicious attack on the business.

2.5 Review and revise
Food defence plans should be reviewed and updated regularly. A security breach or suspected breach may indicate that the threat assessment needs revision. After an incident has occurred, it is constructive to review the event and reflect on the response management. Learning from this process can be used to update the threat assessment, amend control measures, and improve response plans.

In addition, food businesses should monitor national and international sources of intelligence on emerging food threats. This can be considered a form of horizon scanning and used to update threat assessments on an ongoing basis.

- Food and Grocery Sector Group (FGSG) of the Trusted Information Sharing Network (TISN) – information disseminated via Australian Food and Grocery Council (AFGC).
- Rapid Alert System for Food and Feed (RASFF) – publishes an annual report on food safety risks by EU country.

- European Union Agency for Law Enforcement Cooperation (Europol) – publishes the following annual reports: (i) EU terrorism situation and trend report, (ii) serious and organised crime threat assessment, (iii) internet organised crime threat assessment, and (iv) annual Europol review.

- FAO/WHO International Food Safety Authorities Network (INFOSAN) – publishes a biennial report of activities including a synopsis of food safety incidents.

3 Malicious contamination

3.1 What contaminants could be used?

Contaminants can be categorised as biological, chemical, physical, and radiological agents (Table 5). Contaminants that are intentionally introduced to food in a malicious attack may be sourced from the business premises, where there are many potential contaminants with legitimate use, or introduced by the attackers.

3.2 How could fresh produce be intentionally contaminated?

How can GROWERS be targeted?

Sites of primary production are often geographically isolated, spread out, and easy to access. There is generally a low level of surveillance across the site, which means that an attacker may have plenty of time to overcome barriers (like locks), carry out activities unobserved, and remain undiscovered (FDA, 2009). Potential targets to be aware of include:

- Substitution of agricultural chemicals with more toxic chemicals

- Contamination of agricultural water used for irrigation, dilution of chemicals, etc.

- Tampering of equipment, tanks, lines, etc.

Although primary production is vulnerable to attack, the likelihood of widescale public harm resulting from such an attack is thought to be low. This is due to the difficulty of introducing sufficient contaminant in a way that would distribute evenly across a large volume of raw produce. Having said that, fruit and vegetables are more vulnerable than other agricultural products because they undergo minimal processing. If an attack is successful, there are few critical control points for detection or removal of contaminants.

How can PACKERS be targeted?

Facilities for wholesale packing and distribution of produce are generally more enclosed than sites of primary production but may not have fully controlled access. High volumes of vehicle traffic, product receival, loading/unloading, and despatch may enable the introduction of tampered produce, which is then further distributed through the supply chain. Packers should consider whether there are opportunities to deliberately contaminate produce during on-site handling. Postharvest processing operations, if performed, may offer targets for *in situ* attack. These include:

- Substitution of postharvest chemicals with more toxic chemicals

- Contamination of water used for postharvest washing, dilution of chemicals, etc.

- Tampering of grading line equipment

- Introduction of contaminants during pre-packing

The security of the water supply is particularly important in fresh produce, which is minimally processed, and where washing is often the only processing step.

How can PROCESSORS be targeted?

The scope of processing in the fresh produce industry extends to manufacture of fresh-cut

Table 5. Types of contaminant

Type of contaminant	Examples
Biological	Pathogenic microorganisms, parasites
Chemical	Allergens, chemical waste, fertilisers, herbicides, industrial cleaning agents, lubricants, mycotoxins, pesticides, veterinary medications, other hazardous chemicals
Physical	Glass, metal, plastic, needles, razorblades, sand, grit, other foreign matter
Radiological	Radioactive elements

and ready-to-eat products. Processing facilities are typically enclosed with controlled access, which means that attackers are likely to be insiders. Processes that involve mixing, secondary ingredient addition, and bulk liquid handling are critical targets because contaminants can be distributed uniformly throughout produce at these points (FDA, 2009). The air and water systems in processing plants are also potential targets.

3.3 How can I reduce the risks of malicious contamination?

General site security: prevent an attacker from accessing your site

- Establish a perimeter with visible and comprehensive fencing. This may not be feasible if operations are spread out, but is an effective measure for some **production** systems (e.g. glasshouses situated close together) and enclosed **packing** and **processing** facilities.

- Install security cameras to monitor and record activity at vulnerable and low observation areas. Conventional CCTV systems may be effective at enclosed **packing** and **processing** facilities. Wireless, long-range, wifi-enabled, solar-powered options are particularly useful for **remote/on-farm surveillance**.

- Situate vehicle parking outside your perimeter (or at least away from vulnerable areas) and monitor access points. Visitors should not be able to enter your site and move around unobserved.

- Schedule deliveries and check documentation. Investigate missed deliveries.

- Only allow visitors by appointment and check proof-of-identity. Ensure visitors are always signed in and accompanied on site.

- Implement a positive identification procedure for staff and visitors (e.g., ID badges, coded hi-vis vests) to improve detection of unauthorised personnel and suspicious activity. This may be particularly useful where there is a large workforce, many casual/seasonal workers, many visitors, or high levels of activity.

- Prohibit staff from bringing personal items into critical areas. Provide changeroom facilities and require personal clothing be separated from workwear.

Credit: ChameleonsEye / Shutterstock.com

Controlled access: prevent an attacker from accessing potential targets

- Store chemicals safely and securely (e.g. under lock).
  - Agricultural chemicals, e.g., pesticides, herbicides, fertilizers
  - Postharvest chemicals, e.g., sanitizers, fungicides
  - Industrial disinfectants and cleaning agents

- Secure water sources (e.g. tanks) with physical barriers (e.g. gates, locks).

- Secure critical equipment that could enable the introduction or distribution of a contaminant in your product.
  - **Growers:** equipment for irrigation, spray applications
  - **Packers:** equipment for washing, postharvest treatments, pre-packing
  - **Processors:** equipment for washing, mixing, staging, reworking, ingredient addition

- If you do secondary food **processing** (e.g. fresh-cuts, salad mixes), store any bulk liquid and secondary ingredients securely.

- Restrict access to critical areas, and operation of critical equipment, to authorised personnel only. Your choice of lock system should be proportionate to risk, e.g., an electronic identity-and-access lock system offers greater security (and assists in identifying an attacker) than an old-fashioned lock-and-key.

- Install alarms and surveillance cameras to monitor potential targets.

Personnel security: prevent an insider threat

- Do pre-employment checks when hiring staff or engaging contractors (e.g., proof of identity, proof of qualifications).

- Be sensitive to staff morale, wage, and labour issues.

- Set up whistleblowing arrangements (see ASIC for advice).

- Follow fair and professional practice throughout the employment cycle, from recruitment to termination (see Horticulture code of conduct and Employment NZ for advice).

- Foster an effective security culture in your business, where staff are not only compliant, but engaged and alert to food defence issues. (see CPNI for advice)

Tamper detection: mitigate the consequences of an attack

- Enhance your ability to detect suspicious activity.
  - Peer monitoring (buddy) system, i.e., staff work in teams rather than alone.
  - If you are responsible for distribution, use GPS/RFID to track vehicles and dedicated trip plans with scheduled stops at well-lit public locations. Require regular driver check-ins and reporting of unscheduled stops.

- Enhance your ability to identify products that have been tampered with.
  - When receiving deliveries (e.g., chemicals, ingredients), check the integrity of packaging and documentation.
  - When receiving or despatching raw or processed product, check product, packaging, and documentation integrity before loading/unloading trucks.
  - Use numbered (tamper evident) seals on hazardous materials and bulk storage containers.

Management practices: systematically support your food defence plan

- Ensure that control strategies are operating as intended with appropriate verification and recordkeeping procedures.

- Check that traceability systems are working effectively as these are pivotal to timely incident response and product recall.

- Arrange food defence training for staff and regular refresher courses to maintain awareness of security issues.

- Arrange simulations/drills to test and refine food defence plan and to practice incident and emergency response protocols.

3.4 What do I do if my produce has been tampered with?

- The response to food tampering needs to be swift and well-coordinated, to minimise harm to the public and costs to the business.

- Alert your local police department and home state food safety regulatory authority (Table 6), who will coordinate an **investigation**.

- Depending on the nature of the attack, it may be necessary to implement an **emergency response** (e.g. evacuate, notify emergency services, request medical assistance) to avoid harm to employees (see Safe Work Australia and business.govt.nz advice).

- Conduct a **product recall**, as agreed with your local police and home state food safety regulatory authority (Table 6) to stop the sale and distribution of tampered product (see FSANZ and NZ Food Safety advice).

- Implement **business continuity** plans including agile leadership (e.g. incident management group, tactical response groups), crisis communication strategy, countermeasures (e.g. enhanced quality monitoring), contingency strategies (e.g. activate backup/recovery systems, outsourcing, adjusting supplier arrangements). (see AS/NZS 5050; business.gov.au and business.govt.nz also have advice).

Table 6. Notify local authorities if you detect/suspect malicious contamination

	Law enforcement	Food safety enforcement
ACT	ACT Policing	ACT Health
NSW	NSW Police	NSW Food Authority
NT	NT Police	NT Health
QLD	QLD Police	Safe Food QLD QLD Health (must be informed of tampering in QLD)
SA	SA Police	SA Health
TAS	TAS Police	TAS Health
VIC	VIC Police	VIC Health
WA	WA Police	WA Health
NZ	NZ Police	NZ Ministry of Primary Industries

The FPSC is providing these fact sheets to translate relevant published research for the Australia and New Zealand fresh produce industries.

Fresh Produce Safety Centre Australia & New Zealand

Room 517, Level 5, Life Earth & Environmental Sciences Building, F22

The University of Sydney, NSW 2006 Australia

E: info@fpsc-anz.com

W: https://fpsc-anz.com

Twitter: @safeproduceANZ

FRESH PRODUCE SAFETY CENTRE
AUSTRALIA & NEW ZEALAND

FOUNDING PARTNERS

THE UNIVERSITY OF SYDNEY

pma AUSTRALIA+NEW ZEALAND