ALLIANCE™
(https://debug.globalseafood.org)

Responsible Seafood ADVOCATE

Responsibility

Beyond HACCP: Total procedures manuals, Part 3

1 April 2005
By Monica Drazba

Bioterrorism and preventing malicious acts

Fences, gates, and regular security procedures help prevent malicious activity at aquaculture facilities.

It is the responsibility of shrimp processors to consider the safety and purity of the products that come from their plants. Unfortunately, world political events have made it clear that processors must look beyond accidental adulteration and think about malicious tampering or contamination.

Although HACCP is a tool all processors effectively use to combat microbiological and chemical contamination, it is not perfectly suited to the prevention of malicious acts. But that is not to say HACCP principles can't be used to analyze potential malicious hazards and develop prevention and mitigation procedures that build on routine food safety procedures to assure total procedures manuals that encompass malicious risk prevention and mitigation.

As in HACCP, the first steps in developing a plan to prevent malicious acts or bioterrorism are consideration of the risks that can occur, and where, when, and how they can occur, then determination of the physical needs and procedures required to prevent or mitigate the adulteration. And also like HACCP, a team approach is generally the best option for this process. After the security plan is in place, a security team can also review routine inspection reports, make recommendations for improvements, and serve as an investigating body to determine the source of any malicious tampering.

Once the team has identified physical and operational weak areas, the next logical step is to strengthen the debilities. In general, this takes two directions: assessing and then improving physical security, and adding or improving operating procedures to ensure that malicious acts can't take place.

Physical security

Assuring physical security is fairly straightforward and at a minimum should include sufficient perimeter security, lighting, and water source and access controls. Fences should be high enough and strong enough to prevent entry, and inspected and maintained regularly. Security lighting, which should illuminate most areas of the plant grounds, should also be monitored, with burned-out bulbs replaced immediately. Access points should be designed to ensure that guards can control who enters and leaves. These, too, must be inspected and maintained to ensure they are effective.

Procedures for inspections and security checks of grounds perimeters, buildings, and other areas should be outlined in total procedures manuals, and include the frequency of inspection walks and reporting mechanisms.

Fences and Walls

Plant grounds are fenced to prevent the entrance of people or animals. A maintenance team should walk along the fence during routine daily checks to assure the integrity of the physical barrier. Guards who carry out perimeter checks should also note any anomaly in fence security in their shift logs and report them to security supervisors. If fencing is broken or indicates signs of tampering, the maintenance chief should immediately report the problem to the operations manager and security chief, and fix it as soon as possible.

Water

Because the water used in processing plants represents a large potential hazard for contamination, it is very important to ensure that water sources are secure. If a plant has its own well, the well, pump, and water storage areas should be fenced. Access to this area must be limited to the appropriate personnel.

Guards

Once physical security considerations are addressed, operations must be reviewed in light of possible bioterrorism. Security operations can include guarding activities, visitor and employee access controls, loading procedures, and information management.

The guard forces for processing plants should be trained initially, then provided with training updates to maintain high performance standards.

Guards should receive two kinds of training: internal plant procedures and responsibilities, and biannual training for vigilance personnel provided by national army or police personnel contracted to improve guard performance. Human resources records should be kept of the training, with all guards receiving both internal and external orientation at least once each year.

Limiting access

Limiting employee and visitor access is also important to the control of hazards. The processor should consider employee background, provide identification badges, color coded uniforms and a variety of other actions to ensure that employees and visitors are not able to wander at will around plant environs. See the following short excerpt:

Employee security

All prospective employees should provide work references, addresses, or other contact information. They should also provide official documents that state they have no criminal record.

All employees should be issued identification badges, which must be presented to enter plant grounds and worn at all times (under work aprons in processing areas). Badges should be color coded, with permission for access to certain areas of the plant grounds defined by a color coding system.

Personnel who enter areas to which they are not usually allowed access should show a work order or permission slip from the operations manager, maintenance manager, or general manager of the plant.

Sanitary operating procedures also mandate color-coded work uniforms based on area, so workers must stay within their designated plant areas. Employees should receive basic orientation on general security procedures as well as job responsibilities, and understand the importance of reporting any suspicious behavior on the part of other employees, visitors, or service providers.

Visitor access

Visitor access must be controlled rigorously, with badges and accompanying employees required. Visitors who routinely spend time in plants should be issued permanent badges with the same restrictions that apply to full-time employees.

Loading and other areas where products might be prone to tampering should be well guarded and have limited visitor access. Given the value of final products, plant procedures at this point are usually already sufficient to prevent tampering. Should a problem occur, the recall procedures necessary to HACCP plans should be implemented immediately.

Record keeping

As in HACCP plans, maintenance and operational activities should be documented with records that verify security procedures are implemented. The importance of record keeping cannot be overstated. Monitoring and documenting actions are the most effective ways for processors to judge the efficacy

of their plant security programs.

During routine meetings, security teams should discuss security issues and assure that procedures are implemented correctly. Should a problem arise, the team can also determine the cause, take actions to report criminal acts appropriately, and recommend changes to procedures or physical plant to prevent further malicious acts.

(Editor's Note: This article was originally published in the October 2005 print edition of the Global Aquaculture Advocate*.)*

Author

MONICA DRAZBA

Mirador de Sto. Domingo #84
Managua, Nicaragua

drazba@cablenet.com.ni (mailto:drazba@cablenet.com.ni)