PROTECTING CRITICAL INFRASTRUCTURE

Molly Cooper investigates how tank terminal operators can protect their staff and assets from terrorism and security threats

IN A TIME where parts of the world are at war, and security threats and terror attacks loom large, safeguarding critical infrastructure becomes vital. This includes storage terminals. 'In any event of any war, the first thing that you attack is the infrastructure. Oil, gas, electricity, water and that's what's happening in Ukraine. They are going to attack what the country is dependent on,' says Chris Phillips, managing director at IPPSO (International Protect and Prepare Security Office).

Storage facilities and refineries cover large areas, while having a constant flow of workers and materials which create significant security challenges. 'Traditionally, security at these sites consists of fences, surveillance cameras, access control and on-site personnel. These measures provide a solid foundation, but security gaps exist,' explains Brad Martin, director of product management at Senstar.

A lack of proper security systems for terminal operators can be very costly. A deliberate attack on a facility could result in injury or loss of human life, harm to the environment and severely impact supply chains. Even less serious incidents, such as theft or trespassing, could also result in damages to high-value assets and interruption of operations.


01

In the last year, *Tank Storage Magazine* reported on many security incidents at tank terminals, including data breaches, tank explosions, refinery fires, drones and war-fueled attacks. Terminal operators must have a comprehensive approach to security, training and anti-terrorism. 'Many terminals are operated reactively rather than proactively,' says Arend van Campen CEO at Tank Terminal Training. This approach needs to be changed as a priority.

REGULATORY COMPLIANCE

In the UK, sites that store certain products above specific quantities fall under COMAH – the Control of Major Accident Hazard Regulations. These regulations are founded on the Seveso directive that underpins European legislation.

Under this legislation, there is a requirement to demonstrate the competence of the workforce across all levels, including coordination with offsite partners. 'Compliance with all of these regulations has two main factors – security and training,' says John Reynolds at Reynolds Training.

Other key regulations for terminals in the sector to consider are:

- Sites served by jetty will need to comply with the International Ship and Port Facility Security Code, which places specific requirements on the port to ensure security is maintained both within the port itself and on the vessel.
- Alarm Management which is underpinned by a set of standards from EEMUA (The Engineering Equipment and Materials Users Association). These standards generally mirror the International Society of Automation standards for alarm management.

PROTECTING EVERYONE

Phillips began his career working at the National Counterterrorism Security Office, a police team whose role was to protect the UK from terrorist attacks. 'This included hazardous sites, terminals, coal and gas sites and protecting places with crowds or large amounts of people. So, I learnt a lot about the industry,' he explains.

Phillips recounts the Buncefield fire incident in the UK and the impact that had on safety and security operations. Although an accident, it showed how much damage a tank explosion could cause. 'It made us realise that a lot of critical infrastructure were actually hazardous sites and were not well protected,' says Phillips.

He recounts a time in which his team were investigating a group of terrorists who were exploring how they could attack a tank terminal in the north of England. While nothing happened, it put in perspective the security measures required for this type of critical infrastructure.

Phillips says, 'Due to situations I had witnessed like this, when I retired, I set up a consultancy for anti-terrorism, security training and help. I've trained many CEOs in the TotalEnergies refineries in counterterrorism and run other training courses at terminals globally.'

WHERE TO START?

Proper security really begins with basic knowledge and research. 'It's really important for people in the oil and gas industry to have knowledge of terrorism, how terrorists choose their targets and what type of methods that they would use to damage or destroy a site,' says Phillips.

'All senior personnel in head office, down to all staff on the ground need to understand terrorism,' he says. This includes how it could impact their business, how they could be a target and also how to ensure that there's a security culture at their sites that protects them from these types of incidents. Health, safety and security must be equal partners.

KEY STEPS

Physical security at tank terminal sites is the first step. But with new and emerging technologies, such as drones aiding attacks, not all physical security features can protect it. 'The fences and the gates can be all 10 ft high with barbed wire on them but if you've got a drone that can fly over the top of it, you need to consider what you need in place to prevent that,' says Phillips.

As a non-profit organisation, IPPSO provides engineered penetration tests on security systems. This tests if the equipment works and if the teams in charge are doing their jobs correctly. 'If we make a breach on perimeter security, we will be looking to see if the camera operator picks it up immediately and reports it through the right processes,' explains Philips.

Cyberattacks can also start from within. IPPSO provides a service which looks at a company's employees and hiring processes, ensuring that companies are doing the right background checks on people when they come to work for them.

Phillips provides five key points that all on-site personnel need to know when it comes to protecting themselves:

- Be aware of the threats
- Understand the motives of potential attacks
- Protect yourselves
- Evaluate potential implications if anything happens
- Test security and run through scenarios

By doing this, companies could save themselves from attacks.

INTELLIGENT MANAGEMENT

'Physical security technology can augment the effectiveness of both physical infrastructure and security personnel. When designed and deployed correctly, it is a cost-effective element of a facility's risk management program,' explains Senstar's Brad Martin. The company is a technology provider in advanced sensing and information management systems for the protection of critical infrastructure and facilities.

On top of the costs, a less tangible side effect is the damage done to a corporation's reputation. Security breaches could lead to a perceived inability of the organisation to foresee and respond effectively to threats. In turn, this could have long-term effects on regulation, future approvals, and public opinion.

THE EQUIPMENT

Senstar provides comprehensive physical security solutions, extending beyond the traditional forms of protection. 'Fence-mounted perimeter intrusion detection sensors turn existing fences into smart fences by detecting and locating attempts to cut, climb, or lift the fence fabric,' says Martin.

When an intruder is detected, the fence generates an alarm and provides the precise location, which can be used to trigger other on-site security resources, including cameras and sirens, loudspeakers, or security lights. The system can be monitored by centralised security personnel, enabling them to assess the situation remotely and dispatch a response if required.

'One question that always gets asked about fence-mounted sensors is what happens if someone cuts the cable? When the sensor cable is cut, either accidentally or in an attempt to defeat the sensor, the system immediately reports the incident, including its exact location,' explains Martin.

A new trend Senstar has seen is in intelligent, lighting perimeter security. This is installed on fences outside of designated hazardous areas. LED-based luminaries provide wide-spectrum illumination targeted along the fence line. 'LED-based lighting is also ESG-friendly and dramatically reduces electrical consumption while a 10-year-plus lifespan eliminates maintenance,' says Martin. Sensors embedded in the luminaries themselves detect the fence vibrations caused by someone attempting to cut, climb or lift the fence fabric. 'Knowing they are detected, potential intruders may rethink their actions.'

MAXIMISING HSEQ & OPERATIONAL EXCELLENCE BY INFORMATION SCIENCE

Tank Terminal Training is a training company focusing on downstream marine storage terminals training and consulting. It develops specific training programmes that help clients boost their professional excellence and HSE standards. During training at Arabian Chemical Terminals in Abu Dhabi, Arend van Campen CEO at Tank Terminal Training, discussed the requirements for total safety and launched Behaviour Observation Teams.

'Every employee, including managers, office staff, operators or contractors, takes part in rotating observation teams of four to six people, observed the day-to-day operations for a period of two weeks,' explains van Campen.

During this time, they list risky behaviours and convene to talk about this with management. These findings allow an HSEQ culture to be built and sustained. Van Campen regards information as being crucial to ensuring work gets done at a terminal. Without information, there will be a shortage of energy, putting the functionality of the terminal at risk. This information theory-based training creates a fair and uniform approach for HSQE culture.

THE POWER OF SENSORS

A large critical infrastructure site was protected with Senstar's Fiber Patrol fibreoptic sensor and Senstar's Symphony video management system (VMS) when an intruder began climbing the fence and it was immediately detected.

In addition to displaying an alarm in the central security office, the VMS automatically zoomed a high-powered PTZ camera to the intruder's precise location for immediate operator assessment.

The barbed wire outrigging on the fence delayed the intruder by snagging them as security personnel went out to the location and apprehended him, before he could reach any sensitive areas.

COMBINING WITH AI

Advances in artificial intelligence (AI) have led to the development of sophisticated object classification capabilities, including people and vehicle types. 'This is important because these software modules may be included as part of a video management system,' explains Martin.

Video analytics can detect and track activity both inside and outside protected zones and can be added onto existing systems at a low cost. Senstar's Sensor Fusion Engine synthesises data from both fence sensors combined with video analytics to increase detection rates in more challenging deployment scenarios.

Martin says: 'For security operators, this helps deal with information overload and alarm complacency – when an alarm occurs, it is real and must be responded to immediately, avoiding any confusion.'

ENSURING PROPER TRAINING

Effective personnel training at storage terminals is critical for safe and efficient operations, reducing the risk of accidents and errors and ensuring highest security standards. 'Training should embed core actions into an individual's mindset. If you've got good emergency response training, it starts to develop muscle memory; what to do, where to go, initial actions to take,' says John Reynolds, managing director at Reynolds Training.

Reynolds Training is focused on the energy sector, and specifically on the development and demonstration of competence across the whole sphere of operational and maintenance requirements within a bulk storage facility.

'This goes from understanding tank farms through to occupational and process safety and control of work. It drives technical competence as well as softer skills around communication, mental health and people management,' explains Reynolds.

TRAINER TO OPERATOR

As advice from trainer to terminal operator, Reynolds believes in assessing. 'Assess where your vulnerabilities lie. This can be done in a very methodical way,' he explains.

Identify the assets present on site – both hardware and software and the systems that connect them.

Determine possible entry points to these assets and evaluate the level of control within your in-house systems.

Check all software is up to date and any unnecessary software that can be removed.

Act on findings, update assets, limit access, train personnel in the security of information.

A SECURE FUTURE

'With changing technologies and competing energy sources, we will require new skills and competencies as well as the evolution of the regulatory framework that ensures safety is maintained,' explains Reynolds.

In recent years, cyberattacks have become more sophisticated. These attacks can be Distributed Denial of Service (DDoS), ransomware, malware, insider threats, supply chain attacks when third-party vendors are targeted to gain access, physical attacks with cyber consequences, and vulnerabilities in Internet of Things (IoT) devices.

'As AI advances, potential threats to critical infrastructure include more sophisticated AI-powered attacks. Also, deepfakes can be used to deceive personnel responsible for critical infrastructure,' explains cybersecurity expert at NordVPN, Adrianus Warmenhoven. AI can help hackers to identify and exploit the vulnerabilities that are already present in the company.

Cyberattacks and data breaches can lead to loss of customers' trust and loss of business, further leading to regulatory fines and legal actions. It is important that critical infrastructure companies employ network segmentation to isolate critical systems from less sensitive networks to reduce breach impact.

Warmenhoven says: 'It is key to educate employees about the importance of cybersecurity and make sure that the security practices are updated and advanced regularly. It is also important to have a reliable action plan that would help in case of a breach,'

Regular backups and use of the most advanced cybersecurity tools will help companies to feel ready for possible attacks. This will also help mitigate the impacts of any attacks.

The global economy is in the middle of an energy transition which will have a major impact on terminals. These rapidly emerging fuels will have to work alongside current hydrocarbon based economies, and tank terminal security will need to account for both types of fuels.

For more information:

www.ippso.co.uk

www.nordvpn.com

www.reynoldstraining.com

www.senstar.com

www.tankterminaltraining.com

01 Senstar's LED-based luminares

02 John Reynolds training operators in the Process Centre