IT Security | Supply Chain | OT Security | Insider Threat | Physical Security | Interoperable Communications

ChemLock: Chemical Security on a Budget

Overview

CHEMLOCK

Know your chemicals.
Lock in your security posture.

Whether a small business or an international company, everyone who interacts with dangerous chemicals has a role to play in understanding the risk and taking collective action to prevent chemicals from being weaponized by terrorists. The Cybersecurity and Infrasructure Security Agency's (CISA) ChemLock program is a completely voluntary program that provides facilities that possess dangerous chemicals no-cost services and tools to help them better understand the risks they face and improve their chemical security posture in a way that works for their business model. This resource highlights some simple, effective, and cost-efficient actions to enhance a facility's security posture.

Security Goals

When considering how to optimize chemical security at your facility, it is important to start with an assessment of the different threats and hazards that may affect your facility, the vulnerability of your facility to an attack, and the consequences if the threat were to occur. For example, where are dangerous chemicals located, who has access to them, and how difficult are they to access or remove? Once these risks are assessed, facilities can apply a holistic approach to improve security measures using five security objectives.

1. **Can you DETECT an attack or suspicious activity?**
2. **Can you DELAY the adversary?**
3. **Are you able to RESPOND in a timely manner?**
4. **Are you protecting your CYBER assets?**
5. **Do you have POLICIES, PLANS, and PROCEDURES to implement your plan and security measures?**

Examples of Effective, Cost-Efficient Security Measures

Detection

- Explore opportunities for low-cost video monitoring systems and alarms.
- Train facility personnel on identifying and reporting suspicious activity.
- Develop an inventory control process to routinely check your chemical holdings, including:
  - Maintaining an inventory of quantity and location(s) for each chemical on site.
  - Monitoring frequency of access by authorized personnel.
  - Identifying the process for tracking receipts and chemical shipments as applicable.
- Ensure adequate lighting to deter and detect intrusion attempts.

Delay

- Consider perimeter and asset barriers that delay intruders and increase time for detection and response.
- Store smaller, portable containers of chemicals in cages or defined rooms with secure doors requiring specific keys, access cards, or keypad codes.
- Consider vehicle identification measures for vehicles to access the premises.
- Ensure access points are locked when not in use or manned.

- Implement an identification check at entry points and a visitor escort policy.
- Implement an access control process to limit restricted-chemical access to appropriate individuals.
- If dangerous chemicals are sold, implement a customer verification process.

Respond

- Initiate and maintain a relationship with local law enforcement and first responders that may be contacted in the event of an incident.
- Consider providing facility points of contact and facility layout information—including locations of dangerous chemicals—to local law enforcement and first responders.
- Develop a crisis management plan considering the multiple threats and hazards that may occur.
- Subscribe to and maintain awareness of National Terrorism Advisory System (NTAS) bulletins and notifications (dhs.gov/national-terrorism-advisory-system).

Cyber

- Identify all cyber and information systems that monitor and/or control processes that contain dangerous chemicals, manage physical processes that contain a dangerous chemical, or contain business or personal information that, if exploited, could result in the theft, diversion, or sabotage of chemicals.
- Implement password control and password requirements for systems users. Consider:
  - Requiring password changes at least once every 60 to 180 days.
  - Implementing password protocols to deter easy-to-guess passwords (i.e., 8-character minimum, uppercase and lowercase letters, at least one number and symbol, etc.).
  - Refraining from using shared passwords between users on a common device or system.
- Require two-factor authentication to critical systems.
- Install software patches so that attackers cannot take advantage of known problems or vulnerabilities.
- Install firewalls and anti-malware software to protect local operating systems.
- Back up all critical information, store backups offline, and test backups periodically.
- Provide cybersecurity training to personnel.
- Subscribe to US-CERT cybersecurity alerts at us-cert.cisa.gov/ncas/alerts.

Policies, Plans, and Procedures

- Develop and provide procedures regarding access to chemicals and audit them annually to ensure they are up-to-date. Identify persons responsible for each procedure and ensure they are trained and aware.
- Maintain inventories of key cards, devices, or keys that give access to chemicals.
- Consider implementing background checks on employees with access to dangerous chemicals.
- Conduct a chemical security awareness training for personnel and conduct routine drills and exercises to practice response to facility security incidents.
- Develop and implement policies for inspecting and maintaining security equipment.
- Develop an incident reporting protocol. Ensure incidents are reported to local authorities and to CISA at central@cisa.gov, as appropriate.

Additional Resources

- No-cost ChemLock services and tools: cisa.gov/chemlock
- ChemLock: Secure Your Chemicals: cisa.gov/chemlock-security-plan
- Other CISA services for facilities with dangerous chemicals: cisa.gov/chemlock-cisa-services

Note: Participation in any portion of CISA's ChemLock program does not replace any reporting or compliance requirements under CISA's Chemical Facility Anti-Terrorism Standards (CFATS) regulation (6 CFR part 27). Some ChemLock activities may fulfill CFATS requirements, depending on your specific security plan. Contact local CISA Chemical Security personnel or visit cisa.gov/cfats to learn more about CFATS regulatory requirements.