Invention Journal of Research Technology in Engineering & Management (IJRTEM)
ISSN: 2455-3689
www.ijrtem.com Volume 2 Issue 2 ǁ February. 2018 ǁ PP 30-32

Security in The Chemical Industry

Matthew N. O. Sadiku[1], Sarhan M. Musa[1], and Osama M. Musa[2]
[1]*Roy G. Perry College of Engineering Prairie View A&M University Prairie View, TX 77446*
[2]*Ashland Inc. Bridgewater, NJ 08807*

ABSTRACT: *The chemical industries face many of the same cybersecurity challenges that other industries face. Since chemical industries handle large amounts of hazardous chemicals, they may be of interest to terrorists. The security challenge facing chemical industries today is twofold: designing new systems that meet cybersecurity standards and modifying or modernizing existing systems to meet cybersecurity requirements. This paper provides a brief introduction to security issues in the chemical industry.*

KEY WORDS: *chemical industry, chemical security, cybersecurity*

I. INTRODUCTION

The chemical industry consists of several industrial sectors, including production of chemicals, oil and gas, and the pharmaceutical industry. It also includes manufacturing industries for paints, varnishes, soaps, detergents, cosmetics, etc. The chemical industries manufacture chemical products that are critical to the life, health, and well-being of people across the globe. They have thousands of facilities that use, manufacture, and store chemicals, encompassing everything from petroleum refineries to pharmaceutical manufacturers to hardware stores. They play an important role in the US economy by producing goods and services and employing citizens. Because of their critical economic role and their responsibility to their employees and society, security is a top priority.

The general consensus is that some US chemical facilities are vulnerable to terrorist attacks. In recognition of the risks chemical industries pose, US Congress passed a rule known as Chemical Facility Anti-Terrorism Standards (CFATS), which currently regulates all aspects of chemical security. The goal of CFATS is to secure US chemical infrastructure against potential terrorist attacks [1]. As part of the overall strategy for preparing and responding to terrorist attacks, chemical companies are encouraged to develop counterterrorism and security protections. Cyber attacks are real; they come from various sources such as viruses, worms, trojans, hackers, a disgruntled employee, or terrorists [2]. Cybersecurity is critical to the success of any chemical company; it keeps chemical processes working safely and ensures that data is not compromised.

II. SECURITY

Security is being protected against the potential danger or loss that can result from the intentional acts of others. It involves taking all preventive measures to avoid harmful incidents caused by unauthorized (internal or external) persons who intend to seriously damage the company [3]. It is preventing intentional or unintentional interference with the proper operation of industrial automation and control systems. Security and safety are closely related concepts. Security is protecting a computer system against the threats of the external environment, while safety is protecting the environment from potential dangers of a computer system [4]. Like safety, security must be an integral part of any chemical process. Every company needs a security policy which should be implemented in a proactive way and even be part of their mission statement. The company may also need to have security countermeasures in place.

Cyber attacks are threatening the operation of businesses, banks, companies, and government networks. They vary from illegal crime of individual citizen (hacking) to actions of groups (terrorists). Typical examples of cyber attacks or threats include malware, phishing, denial-of-service attacks, social engineering attacks, and man-in-the-middle attack. Cybersecurity is the process of protecting computer networks from cyber attacks or unintended unauthorized access. The security objectives have been availability, authentication, confidentiality, nonrepudiation, and integrity [5].

III. ACHIEVING SECURITY

There are several ways the chemical industry can enhance security. These include physical security enhancement, protecting workers and the environment, regulation, and collaboration with others.

- **Physical security enhancement:** Site security can be improved by "hardening" defenses so that sites would be less vulnerable to terrorists. Protecting the chemical facilities, information regarding chemical formulas, and customer databases, from potential cyber-attacks, is crucial. Building such a security culture within a chemical plant, in addition to safety culture, may be essential for preventing unwanted intentional events.

- **Protecting workers:** Occupational Safety and Health Act (OSHA) has issued several standards designed to protect workers. Employers must provide its employees with a workplace free from chemical hazard, which is a set of circumstances that may result in harmful consequences. Each chemical industry must ensure that workers, the public, and the environment are protected from unreasonable risk resulting from accidental and intentional chemical releases. It may be necessary to train employees some specific skills such as emergency response, bomb threats, hostage situation, first aid, etc.

- **Regulation:** Regulations should continue to require facilities to meet stringent security standards. To secure chemical facilities, the federal government must provide regulatory certainty. The Department of Homeland Security (DHS) should address this issue and ensure that all high-risk chemical facilities are safe, secure, and fully comply with CFATS. A variety of federal policy options can be used for chemical security.

- **Collaboration:** Leaders in the chemical industry are stepping up efforts with an alliance previously formed, the Chemical Sector Cyber Security Program (CSCSP), to maximize cyber-security. CSCSP was established in 2002 and based in Arlington, Va. CSCSP hosts two general meetings each year. It is designed to enhance cyber security throughout the chemical sector and develop strategies to protect people, property, products, processes, information and information systems. Its mission is to develop a sector-wide strategy to address cybersecurity issues and align the chemical industry's priorities with those of DHS.

The CSCSP includes five key initiatives [6]: (1) fostering involvement and commitment across the sector; (2) establishing a program to advocate the establishment of sector practices and policies; (3) establishing sector practices and standards; (4) establishing an information sharing network; (5) and encouraging acceleration of improved security technology and solutions development. To achieve its mission, the CSCSP needs partner with business, industry, and vendors.

IV. CHALLENGES

There are several challenges in dealing with security issues in the chemical industry. Setting up a secure anti-terrorism policy and security culture is costly. Security management needs to provide top management with detailed security cost and benefits figures [7]. Because cybersecurity is not well-understood by non-experts, the economics are hard to demonstrate, and effectiveness is difficult to measure. Wireless connection makes industrial systems vulnerable to security intrusions. There is the shortage of cybersecurity professionals. Cybersecurity policy lags technological innovation. Information technology changes rapidly, with security technology and practices evolving even faster to keep pace with changing threats.

V. CONCLUSION

The chemical industry plays a vital role in the lifeline of our economy. Any disruption is likely to cause significant damage both physically and financially. After the events of September 11, 2001, the chemical industry, particularly chemical plants, realized the necessity for increased terrorism prevention. So far, there have been few terrorist attacks on chemical facilities. Evidences of secure working environments are found in almost every chemical plant. More information regarding chemical security can be obtained from the Security Journal and the Journal of Applied Security Research, devoted exclusively for security-related issues.

REFERENCES

[1] A. A. Sadiq, "Chemical sector security: risks, vulnerabilities, and chemical industry representatives' perspectives on CFATS," Risk, Hazards & Crisis in Public Policy, vol. 4, no. 3, April 2014, pp. 164-178.

[2] S. Bajpai and J. P. Gupta, "Site security for chemical process industries," Journal of Loss Prevention in the Process Industries, vol. 18, 2005, pp. 301–309.

[3] G. L.L. Reniers, "Security within the chemical process industry: survey results from Flanders, Belgium," Chemical Engineering Transactions, vol. 26, 2012, pp. 465-470.

[4] A. J. Kornecki and J. Zalewski, "Safety and security in industrial control," Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research, April 2010.

[5] M. N. O. Sadiku, S. Alam, S. M. Musa, and C. M. Akujuobi, "A Primer on Cybersecurity," International Journal of Advances in Scientific Research and Engineering, vol. 3, no. 8, Sept. 2017, pp. 71-74.

[6] "Chemical industry and IBM join forces to improve cyber-security," false Business Wires, January 2003.

[7] G. Reniers, "Terrorism security in the chemical industry: Results of a qualitative investigation," Security Journal, vol. 24, no. 1, 2011, pp. 69–84.

AUTHORS

Matthew N.O. Sadiku is a professor in the Department of Electrical and Computer Engineering at Prairie View A&M University, Prairie View, Texas. He is the author of several books and papers. His areas of research interest include computational electromagnetics and computer networks. He is a fellow of IEEE.

Sarhan M. Musa is a professor in the Department of Engineering Technology at Prairie View A&M University, Texas. He has been the director of Prairie View Networking Academy, Texas, since 2004. He is an LTD Sprint and Boeing Welliver Fellow.

Osama M. Musa is currently Vice President and Chief Technology Officer for Ashland Inc. Dr. Musa also serves as a member of the Advisory Board at Manhattan College's Department of Electrical and Computer Engineering as well as a member of the Board of Trustees at Chemists' Club of NYC. Additionally, he sits on the Advisory Board of the International Journal of Humanitarian Technology (IJHT).