Invention Journal of Research Technology in Engineering & Management (IJRTEM)
ISSN: 2455-3689
www.ijrtem.com Volume 2 Issue 1 ǁ January. 2018 ǁ PP 17-20

Cybersecurity for 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: *Cybersecurity risk pervades all sectors of the US economy. It challenges the reliability, resiliency, and safety of our infrastructures. The chemical industry, particularly the petro-chemical industry, is a critical infrastructure that is vulnerable to cyber attacks. By its nature, the chemical industry deals with products that are sometimes highly hazardous for people and the environment. Cyber attacks on chemical industry represent a threat beyond the boundaries of the factory involved. This paper presents a brief introduction to how cybersecurity affects the chemical industry.*

KEY WORDS: cybersecurity, computer security, chemical industry

I. INTRODUCTION

The Internet presents significant risk as it is open to all kinds of users, misuses, terrorists, spies, and identity thieves. Of significant concern are weapons of mass disruption, not weapons of mass destruction [1]. Terrorists can wipe out our power grid, telecommunication infrastructure, or banking system. We are at risk because America increasingly relies on computers and computer networks. Even people who do not own a computer are subject to disruption since malicious actors can cause them harm by remote control [2].

Security experts have repeatedly warned that the industrial sector, where computer-controlled equipment is commonplace, and other critical infrastructure are vulnerable to cyber attacks. Based on the warning and advice, big national and international companies have started to recognize that the stakes are high. Industrial leaders are stepping up efforts with an alliance previously formed, the Chemical Sector Cyber Security Program, to maximize cybersecurity.

The chemical sector has been identified by the homeland security as a very sensitive sector in terms of cybersecurity. The Chemical Industry Data Exchange (CIDX) developed guidance documents to provide a best practice on cybersecurity in the chemical industry [3]. It ceased to exist in 2008. Cybersecurity should be of interest to the chemical industry because chemical facilities are vulnerable to a terrorist or cyber crime, which can directly affect its business operations. Chemical industries should regularly defend information security threats, including corporate espionage and the theft of intellectual property.

Unlike many other critical infrastructure sectors, the federal government regulates cybersecurity for the chemical industry. Under the Chemical Facility Anti-Terrorism Standards (CFATS), chemical facilities must meet comprehensive cybersecurity requirements that address the protection of business networks and process control systems. Besides CFATS, the chemical sector has also been actively engaged with the federal government as the National Institute of Standards and Technology (NIST; Gaithersburg, MD; www. nist.gov) [4]. They are working with NIST on developing and implementing the cybersecurity framework. This joint effort will lead into a voluntary, risk-based set of standards and best practices to help organizations, regardless of their sizes, security risk, or current level of cybersecurity sophistication, manage their cybersecurity risks [5]. President Barack Obama issued an executive order in February 2013 for the NIST to work with industry to create a voluntary set of cybersecurity best practices to help prevent hacker attacks on critical computer systems [6].

II. OVERVIEW OF CYBERSECURITY

Cybersecurity is the process of protecting computer networks from cyber attacks or unintended unauthorized access. Cybersecurity is focused in a variety of areas such as military, law enforcement, judicial, commerce, infrastructure, interior, intelligence, and information systems. It is a dynamic, interdisciplinary field involving information systems, computer science, and criminology. The security objectives have been availability, authentication, confidentiality, nonrepudiation, and integrity.

Cyberattacks 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). Cyberattacks or threats include malware, phishing, denial-of-service attacks, social engineering attacks, and man-in-the-middle attack. Cybersecurity involves reducing the risk of these cyber attacks. Cybersecurity is the joint responsibility of all relevant stakeholders including government, business, infrastructure owners, and users. Governments and international organizations play a key role in cybersecurity issues. Securing the cyberspace is of high priority to the Department of Homeland Security (DHS). The DHS has a dedicated division responsible for risk management program and requirements for cybersecurity called the National Cyber Security Division. The Federal Communications Commission's role in cybersecurity is to strengthen the protection of critical computer networks and networked infrastructure. The Computer Fraud and Abuse Act (CFAA) remains the most relevant applicable law expressing the U.S. proactive cybersecurity effort [7].

III. CYBERSECURITY APPLICATIONS

Here we consider some useful applications where cybersecurity is required [8]:

(1) Online Identity Theft: Online attackers attempt to steal users' identity during a bank or commercial transaction by impersonating identities of others. Digital identity may contain some sensitive information which can be targets of attacks. Cyberspace is an opportunistic place for identity theft. Digital identity becomes a source of anxiety as people online plunder bank accounts, steal identities, or commit fraud. As digital identity systems become more global and complex, there is a decrease in trust [9].
(2) Industrial Attacks: Attackers seek valuable intellectual properties of companies stored in corporate networks.
(3) Critical Infrastructure: Our adversaries are after destroying our critical infrastructures such electric power grid, chemical refineries, and communications systems.

IV. CYBERSECURITY STRATEGIES

Despite government's involvement in cybersecurity, it is the duty of the chemical sector to implement the measures and strategies needed to mitigate cyber risks. Each company should establish a cybersecurity policy and implement a real strategy regarding cybersecurity. The following guides are offered for mitigating cybersecurity risks.

- Detecting intrusion: The chemical industry's network systems will have to be able to optimize their network detection. It should prevent against data leakage using defensive strategies that prevent breaches of security. A system should always be protected from unwelcome visitors accessing it. It is highly recommended that a single sign on and password is given for each user to access all they need. A defense strategy must take a multi-layered approach to cybersecurity. No single security measure is good enough to prevent intrusions. A defense-in-depth strategy involves layers of protection on assets, intrusion detection, and continuous monitoring, as shown in Figure 1 [10].
- Supporting cybersecurity improvements: The proactive support of cybersecurity in the long run will require a strong and lasting commitment of resources, some clear goals, and close collaboration between the sector's stakeholders. Chemical industry trade associations have launched different cybersecurity programs to help their members improve cybersecurity, comply with federal regulations, and mitigate vulnerabilities to cyber attacks.
- Protecting operations: To make the industry more resilient to cyber attacks and better able to protect our interests in cyberspace, the industry must create a culture for security through on-going awareness campaigns that will protect the business. Security requires an ongoing effort and must be continually managed through the lifecycles of any company. Engineers must ensure that availability, integrity, and confidentiality (AIC) are fully implemented within the overall system approach. For IT, confidentiality is king.

A proactive approach to dealing with cybersecurity attacks must involve a cost-effective and realistic approach that works for the employers and employees.

V. CHALLENGES

Cybersecurity risks are not easy to address and regulate due to the increasing complexity of the network (proliferation of open-source software in industry) and sophistication of cyber attackers. The pace of change in the area is dauntingly fast. The problem is simply too hard for any one industry or government to solve on its own. There is no one-size-fits-all approach to cybersecurity regulations. The US federal government applies a

sector-specific approach to cybersecurity regulations. Cybersecurity measure must be carefully applied to preserve privacy, liberty, innovation, and the open nature of the Internet as a communication medium. Some procedures for detecting intrusions raise some privacy concerns. The government cannot search or seize communications content for cybersecurity reasons without violating the Fourth Amendment [11]. Small companies are tempted to adopt commercial off-the-shelf-technologies such as Windows and Ethernet based solutions to protect their plant. Although there are many advantages to such systems, such 'standard' systems are easier to attack.

VI. CONCLUSION

Cybersecurity threats are real and they happen to individuals in all walks of life on a regular basis. Professional hackers, either for illegal gain or on behalf of unscrupulous countries, are actively masterminding cybersecurity attacks on chemical companies. The consequences of cyber security incidents are diverse and costly. For chemical manufacturers, for example, the consequences can range from production interruption, reputation loss, supply chain impact, and the expense of retrofitting security after an incident. Cybersecurity has now become a national imperative and a government priority. The US government, at the state and federal levels, is committed to prosecuting cyber crimes and holding those accountable for perpetrating acts. However, the private sector is still responsible for the security of their private networks.

REFERENCES

[1] M. J. Cetron and O. Davies, "World War 3.0: Ten critical trends for cybersecurity," The Futurist, September-October 2009, pp. 40-49.

[2] M. Warner, "Cybersecurity: A pre-history," Intelligence and National Security, vol. 27, no. 5, 2012, pp. 781-799.

[3] R. D'Aquino, "Chemical cybersecurity: a work in progress," Chemical Engineering Progress, vol. 101, no. 1, January 2005, p. 7.

[4] S. J. Shackelford et al., "Toward a global cybersecurity standard of care? Exploring the implications of the 2014 NIST cybersecurity framework on shaping reasonable national and international cybersecurity practices," Texas International Law Journal, Spring/Summer 2015, vol. 50, no. 2/3, 2015, 59 pages.

[5] "Chemical sector cybersecurity framework implementation guidance," Homeland Security, 2015. https://www.us-cert.gov/sites/default/files/c3vp/framework_guidance/chemical-framework-implementation-guide-2015-508.pdf

[6] G. Hess, "Cybersecurity White House could offer firms incentives to adopt digital defenses," Chemical & Engineering News, vol. 91, no. 33, August 2013, p. 7.

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

[8] T. Moore, "The economics of cybersecurity: Principles and policy options," International Journal of Critical Infrastructure Protection, vol. 3, 2010, pp. 103-117.

[9] M. N. O. Sadiku, M. Tembely, and S. M. Musa, "Identity Theft," International Journal of Engineering Research, vol. 6, no. 9, Sept. 2017, pp. 422-424.

[10] A. Ginter and W. Sikora, "Cybersecurity for chemical engineers," Chemical Engineering, vol. 118, no. 6, June 2011, pp. 49-53.

[11] G. T. Nojeim, "Cybersecurity and freedom on the Internet," Journal of National Security Law & Policy, vol. 4, 2010, pp. 119-137.

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).

Figure 1. Defense-in-depth approach to security [10].