CHEMICAL ENGINEERING TRANSACTIONS

VOL. 82, 2020

A publication of AIDIC
The Italian Association
of Chemical Engineering
Online at www.cetjournal.it

Guest Editors: Bruno Fabiano, Valerio Cozzani, Genserik Reniers
Copyright © 2020, AIDIC Servizi S.r.l.
ISBN 978-88-95608-80-8; **ISSN** 2283-9216

DOI: 10.3303/CET2082028

Analysis of Past Cybersecurity-Related Incidents in the Process Industry and the Like

Matteo Iaiani, Alessandro Tugnoli*, Valeria Casson Moreno, Valerio Cozzani

LISES – Dipartimento di Ingegneria Civile, Chimica, Ambientale e dei Materiali, Alma Mater Studiorum – Università di Bologna, Italy
a.tugnoli@unibo.it

The process industry and similar sectors are undergoing a digital transition towards higher levels of automation. This, while ensuring advantages such as efficient process control, quick and safe response to abnormal conditions, improvement of product quality and continuous process optimization, it exposes the process sites to cybersecurity threats. A cyber-attack, besides economic and reputation damages, can potentially trigger major accidents (e.g. loss of containment of hazardous materials) with severe consequences on workers, population and the environment.

In the present study, the cybersecurity-related incidents (CSIs) that occurred in the chemical, petrochemical, energy production, and water/wastewater sectors, were investigated. The analysis is based on the development of a database of 78 cybersecurity-related incidents. The aim of the study is to frame a clear picture of the cyber-attacks on IT-OT (Information Technology - Operational Technology) system of process facilities and to issue lessons learnt from past incidents.

1. Introduction

The analysis of external threats faced by the process industry includes intentional interferences, i.e. security threats (CCPS, 2003). Among these, cyber-threats are something that process industry can no longer disregard (Thomas and Day, 2015). This is due to the high level of automation and to the ongoing digital transition. According to a survey from Cisco (Cisco, 2018), 31% of facilities with industrial control systems have experienced a cyber-attack on their Operational Technology (OT) system, while 38% expect attacks to extend from Information Technology (IT) to Operational Technology (Lezzi et al., 2018). A cyber-attack, besides economic and reputation damages, can potentially trigger major accidents (e.g. loss of containment of hazardous materials) with severe consequences on workers, population and the environment, as occurred in 2008 where attackers intentionally induced the explosion of the BTC (Baku-Tbilisi-Ceyhan) crude oil pipeline through remote manipulation of the control system (Department of Homeland Security).

The techniques used to handle security-risks, such as Security Vulnerability Assessment (SVA) or Security Risk Assessment (SRA) techniques (Matteini et al., 2019), typically rely on past event analysis with respect to the phases of identification of vulnerabilities, threat scenarios, impacts and security countermeasures. On the other hand, techniques devoted to cybersecurity of IT-OT systems (e.g. ISO/IEC 27000s series of standards and ISA/IEC 62443 series of standards) refer to the SVA study and incident databases for threat identification.

The current availability of databases reporting cybersecurity-related incidents, populated with data of specific interest for the process industry is still limited. Table 1 reports the studies of some authors who investigated past accidents with a focus on cybersecurity-related incidents: some did not collect incidents that occurred industrial facilities, some show statistical data, only few have investigated the techniques employed by the attackers and no one has analysed the phases of a cyber-attack. In this panorama, the present study aims at collecting and analysing cybersecurity-related incidents (CSIs) that affected facilities of the process industry and the like in the last 20 years. A database of incidents was created, collecting data from a broad set of sources. The data were analysed, focusing on time and geographical trends, impacts of the incidents, and nature of the cyber-attacks (intentional/accidental, CIM level affected). The analysis aimed at pointing out

Paper Received: 9 January 2020; Revised: 27 April 2020; Accepted: 4 July 2020
Please cite this article as: Iaiani M., Tugnoli A., Casson Moreno V., Cozzani V., 2020, Analysis of Past Cybersecurity-related Incidents in the Process Industry and the Like, Chemical Engineering Transactions, 82, 163-168 DOI:10.3303/CET2082028

ongoing patterns in cybersecurity attacks to process industry, also discussing the lesson learnt and the more effective countermeasures.

Table 1: open-source studies on past accidents with a focus on cybersecurity-related incidents

	Considers security-related threats	Considers cybersecurity-related threats	Specific for some industrial sectors	Focused both on IT security and OT security	Statistical analysis of data provided	Investigation of the techniques employed by the attackers	Investigation of the phases of a generic cyber-attack
Vaidya, 2015	✓	✓		✓	✓	✓	
Lezzi et al., 2018	✓	✓	✓	✓		✓	
Nicholson et al., 2012			✓	✓	✓	✓	
French Ministry of Ecology, 2016	✓	✓	✓	✓		✓	
Willems, 2011	✓	✓	✓	✓			
Casson Moreno et al., 2017	✓		✓	✓	✓		

2. Methodology

Two criteria were applied to select the events to be included in the database: i) the event should originate as a result of an intentional or accidental infection of the IT/OT system of a plant; and ii) the event involves an industrial facility belonging to one of the following sectors: chemical, petrochemical, energy production, water/wastewater.

Table 2: definition of the industrial sectors considered and the type of attackers.

	Definition
Chemical	Chemical production and storage installations, including pesticides production, pharmaceutical industry, production of basic chemicals. Transportation and retail of chemicals are excluded.
Petrochemical	Petrochemical production and storage installations, including refineries and oil & gas transportation via pipeline. Other ways of transportation and retail of fuels are excluded.
Energy Production	Electric power production plants using hydrocarbons (petroleum and natural gas based-fuels), hydroelectric and nuclear plants.
Water/Wastewater	Water and wastewater treatment for industrial and domestic purposes. Water supply system is included.
Accidental cyber-attack	A cyber-attack that is not directed towards a specific target, but that infects any vulnerable host. The attacker is generally unknown.
Intentional internal cyber-attack	A cyber-attack that is carried out against a specific target and designed to exploit specific weaknesses of the target system. The attacker is an insider, i.e. an individual who normally has authorized access to the assets of the company (e.g. employee, contractor, business partner, vendor, etc.). The attacker is generally identified by an investigation.
Intentional external cyber-attack	A cyber-attack that is carried out against a specific target and designed to exploit specific weaknesses of the target system. The attacker is not an insider, i.e. he has not authorized access to the assets of the company. The attacker generally claims the attack.

Data were gathered from different sources: scientific literature, the web, open-source databases on industrial accidents (ARIA database (French Ministry of Ecology), RISI database (Department of Homeland Security), GTD (START)). Each entry in the database is structured into fields. Ten "free text fields" allow retaining general details concerning the accident: entry ID number, date, location, affected assets, description of the impacts, implemented countermeasures, description, data source, notes, links. Four "itemized fields" allow to introduce an unambiguous classification of the incidents: industrial sector (chemical, petrochemical, energy production, water/wastewater, all defined in Table 2), type of attacker (intentional internal, intentional external, accidental, defined in Table 2); system infected (IT system, OT system), impacts (IC-01: major accident, IC-02: economic loss, IC-03: PSD/LSD, IC-04: infection of OT system without severe consequences, IC-05: data loss or corruption, IC-06: technical inconveniences at IT level).

The database was analysed in order to obtain statistical data and lessons learned concerning cyber-attacks that involved the process industry and related activities. The analysis concerned the time trend, the geographical location, the distribution among the industrial sectors and the cyber-attack characterisation (i.e. the profile of the attacker, the classes of impacts and the cybersecurity countermeasures).

3. Results and discussion

3.1 Year, location, industrial sector involved and impacts

The cybersecurity-related incidents (CSIs) in the database were first analyzed with respect to time trend (Figure 1a) and geographical location (Figure 1b).

Only 5 events occurred before 1999: this can be justified by the fact that cybersecurity was not a significant threat for process facilities at the time. The time trend shows a peak of the CSIs during the five-year period 2000-2004 (32 events recorded), which is mainly due to the spread of a few very infectious worms (e.g. SQL Slammer, MUMU and Blaster) all over the world. In the last fifteen years, instead, the time trend of the CSIs is constant. Most of the reported events took place in North America (42 CSIs), followed by Europe (15 CSIs) and Asia (12 CSIs). This result could be in part ascribed to the different reporting practices of each geographic area (Casson Moreno et al., 2018). A probable under-reporting concerns Asia, as the continent has the greatest number of process industries (UNIDO, 2019) but less than 20% of the recorded CSIs.

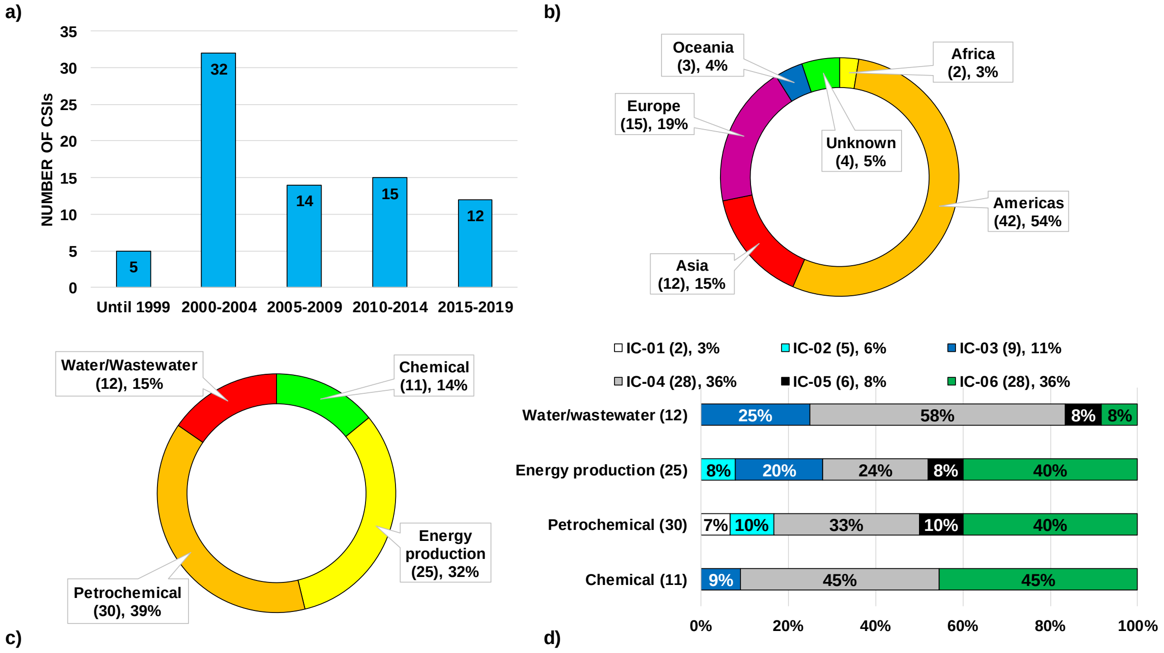

Figure 1: a) Quinquennial trend of the CSIs recorded; b) geographical distribution of the CSIs recorded; c) distribution of the CSIs recorded among the industrial sectors; d) distribution of the classes of impact of the CSIs recorded with respect to industrial sectors. The impact class codes (IC-codes) are defined in Section 2.

Figure 1c reports the distribution of the recorded CSIs among the industrial sectors considered. Petrochemical and energy production facilities were more frequently affected by cyber-attacks (respectively 30 and 25 CSIs). The attractiveness of these installations stems from several aspects: i) the high socio-political impact of the events; ii) the possibility to access proprietary information important for the business (Ackerman, 2004); iii) the high media visibility achievable due to the potential severity of consequences. A lower number of CSIs was recorded for the chemical sector (11 CSIs), in spite of a higher number of chemical facilities over the world (UNIDO, 2019). This may not be explained just as underreporting, and it seems to suggest a lower attractiveness, so far, of chemical industry sites. Finally, 12 CSIs were collected in the water/wastewater sector, almost the same number as those recorded in the chemical sector: this can be justified considering two factors that balance each other: a lower attractiveness ad a higher number of water/wastewater plants than those of the chemical sector.

Figure 1d reports the distribution of the classes of impact with respect to the industrial sectors. The potentially most severe impact (i.e. IC-01) is also the least frequent (only 2 CSIs recorded in the transportation of hydrocarbons by pipeline). No fatalities followed the two major events, however, huge economic losses and environmental damages were reported in these incidents. Generally speaking, the number of recorded CSIs generally increases progressing through the defined impact classes towards those having a lower severity. Large economic losses were reported in a significant number of cases even without a major accident occurring (IC-02). In eight recorded incidents the attackers induced a local or process shutdown via remote manipulation (IC-03). Several cases of infection of the OT (28 CSIs) resulted in no recorded severe consequences. A deeper analysis reveals types of incidents belonging to this category: infection of the SCADA system (21 CSIs), short term loss of plant control (3 CSIs), malfunction of the detection system of dangerous substances (3 CSIs), remote manipulation of plant devices (1 CSI). Most of the CSIs, however, only affected the IT system. Data theft or corruption was recorded in 6 CSIs. The majority of attacks at the IT level only resulted in minor technical inconveniences (server crashes, PC locks, file encryption, etc.).

Figure 1d shows that the distribution of impact classes is similar for all the considered industrial sectors. A few exceptions can be easily explained considering the peculiarities of the sector: e.g. water treatment is expected to have less major accidents (IC-01) and economic losses (IC-02) than other sectors, due to the lower quantities of hazardous materials used and to the lower revenues.

3.2 Characterization and phases of the cyber-attack

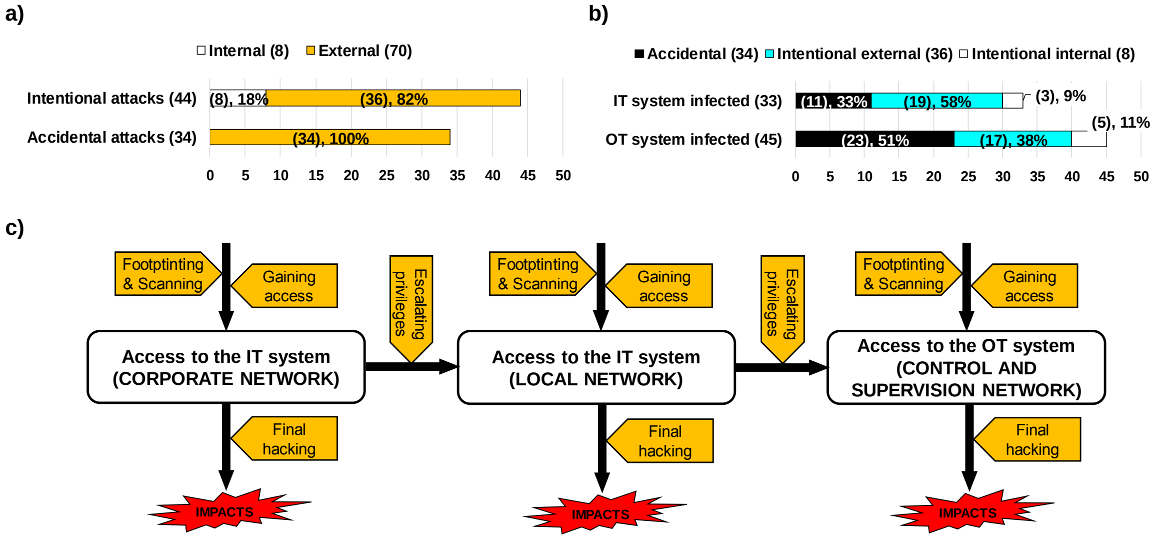

Figure 2: a) Distribution of the CSIs recorded based on the type of attacker; b) distribution of the CSIs recorded with respect to affected system; c) general steps of a cyber-attack to the IT-OT system of a process facility.

Figure 2a shows the overall results of the analysis of the recorded CSIs with concern to the type of attacker (see Table 1). Intentional and accidental CSIs are found to be equally credible patterns (respectively 44 and 34 events). The figure confirms that the external cyber-threat against process facilities is the more frequent CSI reported. Nevertheless, the role insiders is also evidenced as a possible threat (about 10% of the total CSIs recorded). The classification of the collected events with respect to the type of system infected is reported in Figure 2b. As shown in the figure, CSIs that affected the OT system resulted to be more than those that affected the IT system. As an attack to the OT generally implies a former intrusion in the IT system, this result can be a consequence of a higher attention worldwide towards reporting attacks that resulted/may have resulted in physical effects in a facility. Figure 2b also shows that an appreciable number of events classified as “accidental attacks” (i.e. 23 incidents, 29% of the total CSIs recorded), have indeed affected the OT system. A wrong configuration of the IT/OT architecture, especially due to a low attention to security/cybersecurity issues, was tracked as cause of these events.

Generally speaking, the attacker gives rise to a cyber-threat by exploiting vulnerabilities of the target system through one or more hacking techniques. Once a threat scenario takes place, there may be or not direct impacts on the assets of the facility under attack. This depends on the presence and effectiveness of security and safety countermeasures in the system under attack (Henrie, 2013). Footprinting, scanning, gaining access, escalating privileges and final hacking are the well-known steps for cyber-attacks to IT systems.

Footprinting and scanning allow an intentional attacker to collect as much information as possible about the target system, and to identify the vulnerabilities which can be exploited in order to gain the access.

Gaining access to the IT or OT system consists in penetrating the network of the target system through its vulnerable access points. Intentional external attackers obtain the necessary access information by footprinting and scanning steps. The analysis of 8 CSIs with sufficient level of details evidenced that brute force password-cracking, phishing and use of trojan horses are common hacking techniques used by external attackers. Four entries of the database showed that gaining remote access can also involve physical actions on the IT/OT system, most commonly by use of infected USB sticks. Accidental attacks penetrate the IT network when they are able to exploit its vulnerabilities. As regards intentional internal attackers, 8 CSIs were documented in the database as caused by individuals related to the target organization (e.g. employees, contractors, etc.). As insiders usually have extensive knowledge of the process and the plant, they are potentially a very critical category of attackers.

Escalation of the privileges consists in obtaining elevated access to resources that are normally protected from an application or user (e.g. admin, root, kernel resources), in order to manipulate more deeply the system. In particular, this step is necessary to infect the OT system after access is granted to the IT system (see Figure 2c). The network of the OT system is generally a trusted network, separated from the IT system by means of network security systems (e.g. firewalls) (Boudriga, 2010). However, 6 recorded CSIs confirm that a network design lacking of firewalls or with a wrong firewall configuration can result in escalation of the infection spreading from IT to OT systems.

The final hacking is the last part of the cyber-attack, through which impacts on the assets of the affected facility are originated. No recorded CSI with infection of the IT system alone resulted in impacts on the process system, confirming that gaining access to OT is a distinctive feature required to achieve impacts on the physical system in the process industry. The analysis of the 5 CSIs for which more detailed information about the final hacking was available revealed some attack techniques used by the attackers in order to originate impacts on the assets of the target company: Denial of Service, Man in the Middle, and data encryption.

3.3 Countermeasures and lessons learnt

The CSIs for which a more detailed description was available allowed some insights on the key role that security countermeasure may have in preventing such events. The deeper analysis of selected CSIs in the database revealed the following as key countermeasures for those facilities with the network system including both the IT system and the OT system:

- Network segmentation (defense-in-depth strategy): separation between the corporate network and the control and supervision network, allowing their communication only through properly controlled and configured devices (e.g. firewalls).
- Proper configuration of firewalls. In addition to the highly recommended installation of firewalls for data filtering, a proper configuration is important to reduce the possibility of firewalls being bypassed by malware. It mainly consists in establishing which data ports should be closed and which should be open.
- Installation of antiviruses. It is recommended to equip each processor with an antivirus software for the prevention, detection and removal of malwares.
- Authentication system. User authentication is recommended whenever users need to execute actions through a device connected to the network (e.g. by using passwords, tokens, biometric footprints, etc.) and the level of effectiveness of such ways for authentication has to be as high as possible.
- Patch management. It is recommended to install all the available patches in order to update each computer program.
- File encryption. It is recommended to encrypt files and transitioning data.
- Minimizing the use of USB devices. It is recommended to minimize the use of USB sticks since they are the most widely used means for the spread of malware (API, 2003).

4. Conclusions

A specific database was developed and populated with 78 cybersecurity-related incidents (CSIs) that occurred in facilities belonging to the chemical, petrochemical, energy production and water/wastewater sectors worldwide. The analysis of the database showed that in the last 15 years, the number of CSIs has been roughly constant over time, possibly as a result of an increased awareness of companies to cybersecurity issues. Petrochemical and energy production facilities resulted to be the most affected by cyber-attacks: the attractiveness is related to the potential severe impacts that can occur and to the possibility of obtaining proprietary information.

The analysis of the recorded CSIs showed that both intentional and accidental cyber-attacks are credible for such facilities, and that, though external cyber-threats are very credible, an appreciable role of insiders was recorded. The attacks resulted to be able to affect both the IT system and the OT system, which is specific of this sector. The detail available for a sub-set of incidents allowed tracking the general steps of cyber-attacks to process facilities, identifying the phase of accessing the OT system as a distinctive feature of cyber-attacks to facilities belonging to process industry and similar sectors. No specificities were found in the cyber-attacks performed by the attackers with respect to the industrial sectors considered in the analysis.

Some attacks resulted in very severe consequences for the companies affected, as in the transportation of hydrocarbons by pipeline, where two major accidents were induced by remote manipulations of the OT system. Although no fatalities were recorded, huge economic losses, shutdown of process units, loss of process control and monitoring were caused when the control and supervision network were affected by the attackers. Most of the attacks, however, only affected the IT system.

The analysis carried out and the lessons learnt point at defense-in-depth and multiple IT countermeasures as a key-point to hinder and to contrast successfully such attacks. Overall, the results remark the relevance of cybersecurity incidents for the process industry and provides an insight on the patterns of such attacks experienced to date in this specific sector.

Acknowledgments

This work was supported by INAIL (Istituto Nazionale per l'Assicurazione contro gli Infortuni sul Lavoro) in the framework of the 4th SAF€RA call.

References

Ackerman G., Abhayaratne P., Bale J., Bhattacharjee A., Blair C., Hansell L., , A. Jayne, M. Kosal, S. Lucas, K. Moran, L. Seroki, S. Vadlamudi. Assessing Terrorist Motivations for Attacking Critical Infrastructure 2004

API - American Petroleum Institute, 2003, Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries, Washington, API Publication.

Boudriga N., 2010, Security of mobile communications, Boca Taton, CRC Press.

Casson Moreno V., Reniers G., Salzano E., Cozzani V., 2018, Analysis of physical and cyber security-related events in the chemical and process industry, Process Saf Environ Prot, 116, 621–631.

CCPS - Center for Chemical Process Safety, Guidelines for Analyzing and Managing the Security Vulnerabilities of Fixed Chemical Sites, 2003.

Cisco, 2018, Cisco 2018 Annual Cybersecurity Report.

Department of Homeland Security, RISI - The Repository of Industrial Security Incidents.

French Ministry of Ecology, 2016, Cybersecurity in industry.

French Ministry of Ecology, ARIA Database – La référence du retour d’expérience sur accidents technologiques.

Henrie M., 2013, Cyber Security Risk Management in the SCADA Critical Infrastructure Environment, Eng Manag J, 25, 38–45

Lezzi M., Lazoi M., Corallo A., 2018, Cybersecurity for Industry 4.0 in the current literature: A reference framework, Comput Ind, 103, 97–110.

Matteini A., Argenti F., Salzano E., Cozzani V., 2019, A comparative analysis of security risk assessment methodologies for the chemical industry, Reliab Eng Syst Saf, 191.

Nicholson A., Webber S., Dyer S., Patel T., Janicke H., 2012, SCADA security in the light of cyber-warfare, Comput Secur

START, Global Terrorism Database, National Consortium for the Study of Terrorism and Responses to Terrorism.

Thomas H.W., Day J., 2015, Integrating Cybersecurity Risk Assessments Into the Process Safety Management Work Process, In: 49th Annu. Loss Prev. Symp. 2015, LPS 2015 - Top. Conf. 2015 AIChE Spring Meet. 11th Glob. Congr. Process Saf., Austin, Texas, 360–378.

UNIDO - United Nations Industrial Development Organization, 2019, INDSTAD 2 2019, ISIC Revision 3 database.

Vaidya T., 2015, 2001-2013: Survey and Analysis of Major Cyberattacks, 1–25.

Willems E., 2011, Cyber-terrorism in the process industry, Comput Fraud Secur, 2011(3), 16–9.