Chapter 2
Industrial Information Security, Safety, and Trust

Sapna Tyagi
Institute of Management Studies, India

Preeti Sirohi
Institute of Management Studies, India

Mohammad Yahiya Khan
King Saud University, Kingdom of Saudi Arabia

Ashraf Darwish
Helwan University, Egypt

ABSTRACT

The presented chapter elaborates fundamentals issues in information security, safety, and trust in industrial settings. The chapter introduces basics of information security that includes confidentially, integrity, and availability (CIA), which are some of the essential ingredients of information security. The chapter also discusses various reasons for security loop-holes prevalent in industrial setting. A majority of the chapter focuses on security framework and control implementation, which includes various authorizations and authentication methods. The shared secret systems, passwords, token systems, public key infrastructure (PKI), and biometrics system are most common methods used for authentication.

INTRODUCTION TO INFORMATION SECURITY

The industrial information security is the integral part of number theory. The information security in industrial setting is relatively young as an independent discipline. The widespread adoption of information technology has taken place only during the past few decades. Therefore, the security issue has become important for common computer savvy. Earlier, the people uses rely on trust; owners of computer systems hired and controlled the system operators and depended on them to behave in an ethical and responsible manner. (Williams, 2007) The security of data, files, and computer was purely based on the ethical values of a person. But, explosion of internetworking (Internet) and large-scale information systems

DOI: 10.4018/978-1-4666-0294-6.ch002

has rendered earlier approach obsolete. In the networking environment there are many users who share the common resources across the world that leads to the authentication. In general, we can define industrial security as follows:

Industrial Security = Cyber Security + Safety + Physical Security

The industrial security is not mere cyber security but includes safety and physical security. The physical security and safety are equally important for industrial settings. Factories and machine workshops are dangerous places to be and a many accidents takes place every year. The machinery accidents, falls, explosions, burns, chemical inhalation, falling objects, electrocution, fire, etc., are all safety risks in industrial occupations. There is a need to strictly adhere the safety policies and procedures set up in the industrial settings (N. Nagarajan 2009).

The physical security in industrial setting is provided through designated screening or security clearance point. The physical premises may be classified into various zones like Pubic Zones, Reception Zones, Operation Zones and Security Zones (Robert H 2001). The Public Zones include the grounds surrounding a building, public corridors and elevator lobbies etc. A remote surveillance system may install to discourage unauthorized activity in the restricted zones. The Reception Zone is generally located at the entry to facilitate the initial contact between the public and the organization. The Reception Zone also provides a platform where information is exchanged and access to Restricted Zones is controlled. To varying degrees, activity in a Reception Zone is monitored by the personnel who work there, by other personnel or by security staff. While as an Operations Zone is an area where access is limited to personnel who work there. The Operations Zones is monitored periodically based on a type threat and risk assessment. The Secure Zone industrial setting is an area to where access is limited to authorized personnel. A Security Zone need not be separated from an Operations Zone by a secure perimeter. Generally, Security Zones are monitored 24 x 7 x 365 days security staff, other personnel or electronic means. The rest of chapter presents discussion and analysis on cyber security techniques.

Cyber Security

The Internet services provide WWW, e-mails, and other popular services to a base of innumerable users located around the world. The Information for any organizations is most important assets. Therefore, protection of information assets becomes important to establish and maintain trust between the organization and customers. Timely and reliable information is necessary to process transactions and support finances to the organization and customer decisions. The poor information system can adversely affected the earnings and capital by disclosing the information to unauthorized parties, if altered, or is not available, when it is needed (Peter Guerra 2009).

The information security may be defined as a process by which an organization protects and secures the computing systems, storage media, and facilities that processes and maintains information (see Figure 1). Every industry shall maintain effective security programs adequate for their operational complexity. The information security has three primary goals

1. To Maintain the confidentiality of information
2. Integrity, to maintain the intactness of information
3. Availability of information resources when needed.

Confidentiality refers to a mechanism that enforces the secrecy of the data. This is the job of computer security professionals to keep the data safe from unauthorized users. There is variety of techniques that is used to protect data as followings: