Part 1: Introduction, Background, and History of Cybersecurity

1 Purpose of this Book

Cybersecurity has quickly become an essential component in maintaining the safe and continued operations of industrial facilities. A survey of industrial control system operators in 2019 showed that 59% had experienced a cybersecurity incident in the past year [5]. The increase of cybersecurity incidents is not a phenomenon limited to a few specific companies or only the largest corporations. Over the last ten years, numerous attacks on automation systems such as those listed in Figure 1-1 continue to demonstrate that industrial facilities of all types and sizes are vulnerable to cybersecurity attack, and that these cyber-attacks can have significant financial, environmental, and process safety related consequences [6].

Figure 1-1 Major Industrial Cybersecurity Events in the Last Decade

Over the past 20 years, the conversation has moved from "Who could possibly target control systems for a cybersecurity attack?" to a continuing discussion of the many recent breaches and attacks. What has led to this drastic increase in cybersecurity attacks on industrial control systems? The following list provides several factors that could account for this increase:

- Increased interconnectivity of industrial control systems
- Increased convergence of OT and IT systems

- Increased use of Internet Protocol in OT applications
- Increased requirements for remote access
- Increased number of readily available hacking tools
- Desire to target critical infrastructure for political motives
- Increase in number of threat agents with skills to target control systems
- Better identification of cybersecurity attacks
- Increase in known software vulnerabilities
- Increase in known vulnerabilities in legacy systems
- Lack of sufficient cybersecurity awareness and training
- Potential for significant financial gain
- Desire to gain recognition of skills by targeting control systems

While no single cause drives the increase in cybersecurity attacks, it is likely that many of the factors in this list are contributing to the continually evolving cybersecurity landscape.

The purpose of this book is to introduce a risk-based approach for Managing Cybersecurity in the Process Industries and to help organizations design and implement more effective cybersecurity management system programs that are aligned with existing process safety management systems. This approach includes methods for:

1. Understanding cybersecurity risk for the process industry,
2. Integrating cybersecurity management into the existing process safety framework, and
3. Developing a path forward for the future of cybersecurity for the process industry.

The risk-based approach helps to provide an optimum comparison between cybersecurity risk and process risk so that informed decisions can be made. Not all hazards and risks are equal, and it is important to focus time and resources on the higher risks. Cybersecurity risk for the process industry can vary greatly, from potential business impact arising from denial of service or ransomware to the devastating real-world impact of a targeted attack that compromises process control and safety systems. The potential of cybersecurity attacks on the process industry to result in safety consequences

represents a fundamental shift in approach from traditional IT cybersecurity concerns. Adopting this approach for cybersecurity will help all industries that manufacture, use, or handle hazardous chemicals or energy to:

- Develop their approach to cybersecurity incident prevention.
- Continuously improve their management system effectiveness.
- Employ cybersecurity management for non-regulatory processes using risk-based design principles.
- Integrate the cybersecurity business case into an organization's business processes.
- Focus their resources on higher risk activities.

This approach for cybersecurity management builds on the Guidelines for Risk Based Process Safety (RBPS) [7] and the RBPS Management System Accident Prevention Pillars:

Table 1-1 RBPS Accident and Cybersecurity Event Prevention Pillars

RBPS Accident Prevention Pillars	**Cybersecurity Event Prevention Pillars**
Commit to process safety	Commit to cybersecurity
Understand hazards and risk	Understand cybersecurity hazards and risk
Manage risk	Manage cybersecurity risk
Learn from experience	Learn from experience

These pillars remain central for preventing cybersecurity incidents. Leveraging existing risk assessment and management techniques to address cybersecurity reduces the time required to deploy a robust cybersecurity program and improves the alignment between process safety risk management and cybersecurity risk management. The following considerations for cybersecurity outline key steps for addressing cybersecurity risk through the RBPS pillars.

Top management ***commitment to cybersecurity*** is a pre-requisite to successful implementation. Without strong leadership and clear organizational commitment to improving cybersecurity, it is very difficult to make improvements. In addition to driving cybersecurity initiatives, management support is also helpful for establishing a robust cybersecurity culture. Cybersecurity culture is based on awareness (understanding of the cybersecurity impacts of employee actions) and hygiene (understanding of basic security best practices); with these two components in place, conscientious cybersecurity behavior can be promoted. After cybersecurity culture has been established, ongoing management support is critical for sustaining focus on cybersecurity excellence.

Organizations that ***understand cybersecurity hazards and risk*** are better able to allocate limited resources in the most effective way. Due to the many misconceptions about cybersecurity for the process industry, developing an accurate understanding of the potential risks is particularly important. This is a necessary step for incorporating cybersecurity risk into the business plan to lower the overall risk level of the organization and maintain safe and continuous operations.

Managing cybersecurity risk consists of multiple phases including the identification and analysis of cybersecurity risk, designing of cybersecurity protections, implementation of cybersecurity detection systems and procedures for responding to cybersecurity incidents, and recovering from cybersecurity incidents. Strategies such as implementing a cybersecurity lifecycle can help organizations to reduce unexpected downtime and decrease the potential for adverse cybersecurity impacts.

Learning from experience requires monitoring and acting on internal and external challenges. Common internal challenges include previous cybersecurity incidents and near misses, while external challenges include events at similar facilities, industries, technologies, and increased threat activity. Despite an organization's best efforts in implementing cybersecurity management, with the continually evolving threat landscape, cybersecurity attacks are more a question of "when" than "if." Responding effectively to these situations and improving defenses in the future are critical aspects of

cybersecurity management. An effective approach for learning from real world experience is to:

1. Apply industry best practices
2. Correct deficiencies identified from internal incidents
3. Apply lessons learned from other organizations

Monitoring Key Performance Indicators (KPIs) for cybersecurity throughout the life of the facility can provide useful information about how an organization's cybersecurity approach changes over time. In addition to tracking KPIs, periodic audits/ assessments of the current level of cybersecurity drive continuous improvement and sustained results.

The pillars of the risk-based approach for cybersecurity are shown in Figure 1-2:

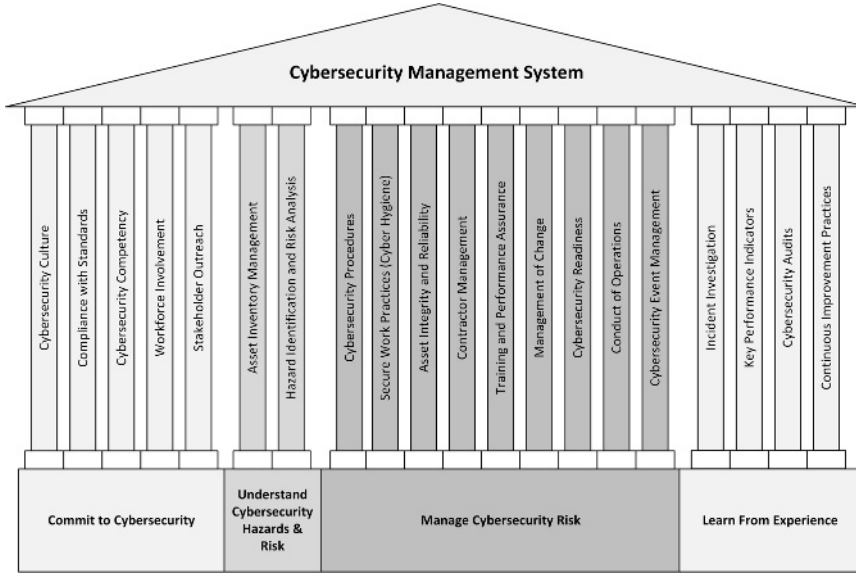

Figure 1-2 Cybersecurity Management System Pillars

Adapted from [7]

Focusing on the pillars of the risk-based approach for cybersecurity should enable an organization to improve its cybersecurity effectiveness, reduce the frequency and severity of cybersecurity incidents, and improve its long-term safety, environmental, and business performance. If the process control system is not secure, it cannot be operated safely. The risk-based approach helps avoid gaps and inconsistencies in the security approach to prevent common cause failures of the control and safety systems.

1.1 Target Audience

This risk-based approach for Managing Cybersecurity in the Process Industries is written for practitioners of the process safety lifecycle including process safety practitioners, process control engineers, instrumentation engineers, maintenance engineers, and process engineers, and others. For simplicity, these roles are referred to as process safety professionals throughout the remainder of this book. Additionally, this book is written for key stakeholders whose decisions can impact the implementation of the process safety lifecycle. The goal of this book is to improve awareness and resilience against cybersecurity attacks by leveraging existing techniques for process safety management. Although process safety professionals have a detailed understanding of process risk and operational technology for maintaining operations, they generally have limited experience with cybersecurity considerations. As such, before diving into the specifics of integrating cybersecurity and process safety management it is necessary to outline the fundamental aspects of cybersecurity.

1.2 What is Cybersecurity?

The IEC 62443-1-1 standard [3] defines security as:

1. Measures taken to protect a system.
2. Condition of a system that results from the establishment and maintenance of measures to protect the system.
3. Condition of system resources being free from unauthorized access and from unauthorized or accidental change, destruction, or loss.

4. Capability of a computer-based system to provide adequate confidence that unauthorized persons and systems can neither modify the software and its data nor gain access to the system functions, and yet ensure that this is not denied to authorized persons and systems.
5. Prevention of illegal or unwanted penetration of, or interference with, the proper and intended operation of an industrial automation and control system.

Essentially, security refers to the ability to protect something from various threats, and cybersecurity is focused on protection from unauthorized access for computer-based systems. Although cybersecurity is a relatively new concept, security in the broader sense has been relevant for as long as there have been things worth protecting.

One common analogy for security is that of the medieval castle. These strongholds of defense were designed with security at their core. The moat, walls, and towers were the measures taken to protect something of value from various threats, such as bandits or attacking armies. This example introduces a key concept for designing with security in mind: defense-in-depth. Defense-in-depth is the principle of maintaining independence across security measures, so that if one layer of defense is compromised, the others remain intact.

Moreover, for a moat to be effective, a drawbridge must grant access to authorized visitors. For security to be maintained, it is important that a gate is also included. This ensures that even if the drawbridge is compromised and cannot be raised, rendering the moat ineffective, the security measures of the wall and gate remain uncompromised.

It is important to note that the defenses of castles only worked until technology advancements such as gun powder and modern weaponry enabled the walls to be breached easily. Similarly, cybersecurity defenses must be maintained and kept technically current; otherwise, they become obsolete and ineffective against attackers.

The three main types of security are physical, personnel, and cyber. These three types of security are closely related and must be implemented together to develop a robust, integrated security policy. It is insufficient to evaluate only one area of security. To truly secure a facility from cyber risk, personnel and physical security must be evaluated in combination with cybersecurity.

1.2.1 What do Process Safety Professionals know about Cybersecurity?

Often when people (including process safety professionals) hear the term cybersecurity, they picture a hooded figure in a dark room "hacking" personal information on an IT network. These "stereotypical" attacks may consist of stealing a user's password using phishing emails (emails designed to trick users into giving personal information and passwords to an attacker) with fake links or attachments that result in downloading/executing malware when clicked. These attacks could lead to identity theft or compromised financial information. Although these are types of cybersecurity attacks that happen on a regular basis, they do not provide the full cybersecurity picture for the process industry. Modern cyber-attacks can go far beyond stealing personal data and have the potential to inflict significant harm on personnel, equipment, and the environment.

A 2014 cybersecurity attack on a German steel mill highlights just how dangerous attacks on control systems can be. Attackers gained access to the corporate network through a phishing campaign intended to compromise operator accounts. They were then able to access the control network and caused multiple process controls to fail. As a result, a furnace at the steel mill was prevented from shutting down, which resulted in significant equipment damage. Fortunately, the site was able to identify the hazardous scenario and evacuate nearby personnel; however, similar incidents of industrial furnaces have resulted in loss of life [8].

1.2.2 What should Process Safety Professionals know about Cybersecurity?

The attack on the German steel mill introduces one of the fundamental differences between Information Technology (IT) and Operational Technology (OT) cybersecurity: attacks on OT can have ***physical impacts***. These differing consequences are a primary driver for the conflicting IT and OT cybersecurity priorities.

For IT security, performance and confidentiality are paramount and outages, while undesirable, are acceptable. This is not true for the process industry, where the need for availability and integrity of the control and safety systems outweighs all other considerations. The priorities are not the only difference between OT and IT cybersecurity, and additional information on these differences is provided in Chapter 8.

Understanding the impact of OT cybersecurity attacks on the process control system is essential for process safety professionals. Particularly striking about the cybersecurity impact on process safety is the possibility for a cybersecurity attack to result in the common cause failure of multiple systems. Industry examples such as the German Steel Mill attack [8], Stuxnet [9], and the Saudi petrochemical facility attack [10] have shown that attackers target both the control and safety/protective functions to achieve the maximum consequence. (Additional information on these and other cybersecurity case studies are included in Chapter 6.) The potential for cybersecurity attacks to trigger the initiating event of a hazard and bypass multiple protection layers can lead to significant unmitigated risk if sufficient security protections are not in place.

Cybersecurity poses new challenges, but by leveraging existing risk assessment and risk management models with new insights, cybersecurity risk can be effectively evaluated. To support this approach, several tools and techniques have been developed for process safety professionals. The following list includes available industry best practice references and regulatory requirements:

- Guidelines for Risk Based Process Safety [7]
- NIST Cybersecurity Framework [11]
- IEC 62443 [12]
- ISA TR84.00.09 [13]
- Chemical Facility Anti-Terrorism Standards: Critical Infrastructure, United States [14]
- NERC CIP: Power, United States [15]
- AWIA: Water and Wastewater, United States [16]

Further discussion of the NIST cybersecurity framework and the IEC 62443 standard is provided in Chapter 7 as a baseline approach for adopting cybersecurity.

In the United States, OSHA's Process Safety Management (PSM) regulation, 29 CFR 1910.119 [17], is often viewed as synonymous with process safety. For many companies in the process industry, application of the IEC 61511 standard is used to demonstrate that OSHA safety requirements related to Safety Instrumented Systems are met. The updated IEC 61511 standard [18] released in 2016 does include new cybersecurity requirements. Any company claiming compliance with the IEC 61511 standard is now expected to complete mandatory cybersecurity activities, including a cybersecurity risk assessment for the Safety Instrumented System (SIS) and all connected networks. Many organizations conduct IT risk assessments of the corporate network, but these studies do not often focus on OT assets such as safety or control systems. As a result, a separate OT focused risk assessment is typically needed to comply with the IEC 61511 requirements.

The growing inclusion of cybersecurity requirements in regulations and international standards serves to underline the fundamental importance of cybersecurity for process safety engineers. Cybersecurity incidents have become a credible threat to controls, alarms, and SIS. Cybersecurity needs to be assessed since attacks can lead to common cause failure for all safety functions (SIFs) in an SIS. Without sufficient cybersecurity protection, traditional protection layers such as Basic Process Control System (BPCS) interlocks, SIS interlocks, and alarms cannot be relied on to raise operator awareness of an unsafe condition or automatically bring the process to the safe state. Simply put - without security, there is no safety.

1.3 What is Operational Technology (OT)?

OT cybersecurity is focused on the protection of operational technology, such as automation systems, industrial control systems, process control networks, and supervisory control and data acquisition systems, from compromise. This book includes information on OT cybersecurity as it relates to the process industry.

Operational Technology (OT) is any hardware or software that detects or causes a change directly to industrial equipment, assets, processes, and

events. Essentially, OT systems are capable of monitoring, controlling, and/or performing safeguarding of physical equipment. Common types of OT equipment/systems include:

- Basic Process Control System (BPCS)
- Safety Instrumented System (SIS)
- Programmable Logic Controllers (PLCs)
- Distributed Control System (DCS)
- Supervisory Control and Data Acquisition (SCADA)
- Fire and Gas Detection Systems
- Allocation and Custody Metering System
- Motor Control Centers (MCCs)
- Burner Management Systems (BMS)
- Building Management/ Automation Systems (BAS)
- Alarm Management System
- Continuous Emissions Monitoring Systems (CEMS)
- Machine Monitoring Systems (MMS)
- Pipeline Leak Detection Systems (PLDS)
- Terminal Automation System

Often, many of these different types of OT components are used in the same OT network to control a variety of different process equipment. Building a reference model, such as the one in Figure 1-3, is often helpful to show the interaction of OT equipment and more clearly illustrate the OT interface with the traditional IT network.

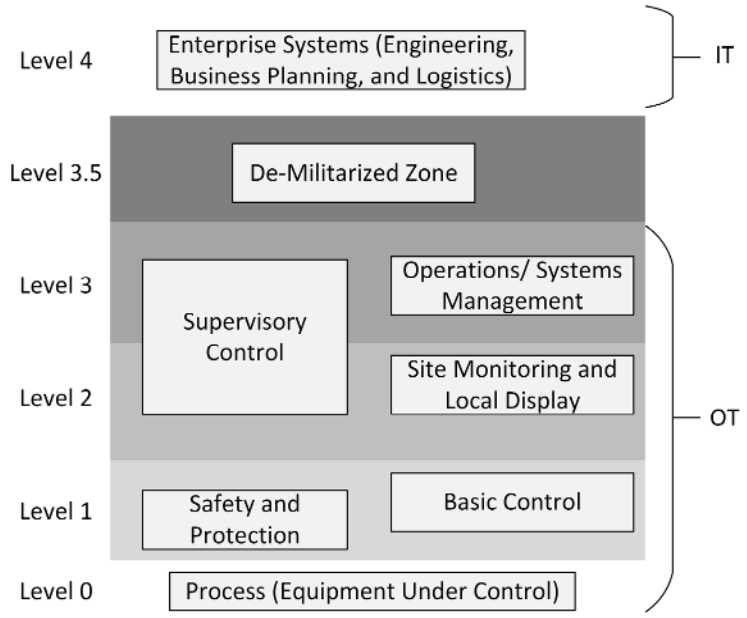

Figure 1-3 OT Reference Model

Source: IEC 62443-1-1 [3]

The traditional OT system is made up of levels 0 through 3:

- Levels 0 (process) contains the physical equipment being controlled or monitored by the OT network (e.g., actuated valve, pressure transmitter).
- Level 1 (basic control) contains the components that interface directly with process equipment, including the programmable logic controllers responsible for basic control (e.g., BPCS, DCS) and for safety and protection (e.g., SIS, BMS, safety PLC).
- Level 2 (area control) contains the site monitoring and local display (e.g., CEMS, operator workstations) that provide additional information about the components in level 1 and 0. Elements of supervisory control (e.g., SCADA) are also considered in this level.
- Level 3 (site operations) contains operations/ systems management that are not directly interfacing with equipment from level 1 (e.g., building management). In some applications, elements of supervisory control are also a part of level 3.

The assets in levels 1-3 have the potential to cause changes at level 0 and affect the physical process; as such, they need to be considered when addressing cybersecurity. When smart devices such as smart transmitters or valve positioners are used in level 0, they need to also be considered in the cybersecurity risk assessment.

Level 4 is composed of the enterprise systems that traditionally make up an internet connected IT network (or corporate wide area network (WAN)/ local area network (LAN)). It is important to protect these systems to achieve overall security; however, these enterprise systems are outside the scope of this guideline.

Level 3.5 (the demilitarized zone or DMZ) is often implemented in networks as a buffer between the IT network and the OT network to prevent direct traffic between the two systems. Often, the ownership of the DMZ is shared between IT and OT teams, and it is an important aspect in securing the perimeter security of the OT network. This is another area where coordination and a close working relationship between IT and OT team members is needed to achieve the organizations cybersecurity goals. More information on the use of a DMZ to improve network segmentation is provided in Chapter 8.

Another term that has become increasingly popular in industry, is Industrial Automation and Control Systems (IACS) . IACS is another name for OT and is defined in the IEC 62443 standard as "a collection of personnel, hardware, and software that can affect or influence the safe, secure, and reliable operation of an industrial process" [3]. It is important to remember that securing the IACS goes beyond just the physical equipment and is dependent on the people and software/ applications as well. All of these areas have to be considered when implementing security protections for the IACS.

1.4 Which industries have OT?

Operational Technology is used in many industries such as chemicals, oil and gas, utilities, and manufacturing. Essentially, any industry where computer systems interact with physical systems uses OT. In some cases, OT is used for control; however, OT can also include monitoring systems for industries that are not typically associated with OT such as building automation systems (BAS), heating, ventilation, and air conditioning (HVAC), fire and gas, and even

transportation systems. Sections 1.4.1, 1.4.2, and 1.4.3 discuss the common OT systems used in various industry groups.

1.4.1 Chemical Processing

Many chemical processing facilities, including petrochemicals, pharmaceuticals, refineries, specialty chemicals, bulk chemicals, and even food and beverage, use OT for critical control and safety applications. In many cases, the control is handled in a connected BPCS or DCS system that may or may not be segmented from a separate safety system or SIS. Numerous real-world incidents have highlighted the potential for consequences resulting from the compromise of chemical processing facilities such as the Saudi Arabia Petrochemical attack [9]. (Additional information on this case study is included in Chapter 6.)

1.4.2 Utilities

Utilities also use OT for a variety of applications, including control and monitoring. While some utilities such as power generation (nuclear, coal, gas, etc.) may have network configurations similar to traditional chemical processing sites, many utility providers such as water supply or natural gas/oil pipelines have much more distributed networks. These networks are often referred to as Supervisory Control and Data Acquisition systems (SCADA). SCADA systems often make attractive targets because of their places in critical infrastructure and the need for everyday activities. SCADA systems need rigorous cybersecurity protection as well and have already been targeted for numerous attacks such as the Maroochy Shire Wastewater incident [19], Ukrainian Power Grid attacks [20] [21], and Oldsmar Water System Attack [22]. (Additional information on these and other cybersecurity case studies are included in Chapter 6.)

1.4.3 Discrete Manufacturing

Manufacturing systems including vehicle production and line manufacturing also rely on OT for essential functions. In many cases, machinery and robotics applications may rely more heavily on segmented OT networks, with PLCs used for control of individual lines or sections of lines. However, even in these segmented networks, growing reliance on digital systems has led to a movement of greater interconnectivity to improve monitoring and advanced control of manufacturing processes.

1.5 Scope

To better focus this information on the most important aspects for process safety professionals, it is important to formally define what is included and what is excluded from this risk-based approach.

1.5.1 Cybersecurity

Cybersecurity is the aspect of security relating to the prevention, detection, and mitigation of accidental or malicious acts on or involving computers and networks. Cybersecurity has multiple focus areas such as IT and OT cybersecurity.

IT cybersecurity is related to the protection of enterprise or business networks that are designed to be connected to the internet. This is the area many people traditionally think of when hearing cybersecurity. The field of IT has been wrestling with cybersecurity for longer than the field of OT, in large part because of the greater interconnectivity of IT systems.

The predominant standard adopted for IT cybersecurity is ISO/IEC 27002:2013, *Information technology - Security Techniques - Code of practice for information security controls* [23], which is a comprehensive catalog of general IT security practices for cybersecurity risk management. IT cybersecurity is primarily concerned with the protection of confidentiality and integrity of internet facing computer systems and often has very different priorities than OT cybersecurity. As such, IT cybersecurity is largely outside the focus of this book.

OT cybersecurity as introduced in Section 1.3 is focused on preventing the compromise of operational technology, such as automation systems, industrial control systems, and process control networks. This book will include information on OT cybersecurity as it relates to the process industry.

1.5.2 Physical and Personnel Security

Three main types/ categories of security are necessary for full protection of assets. These are physical, personnel, and cyber. To truly secure a plant from cyber risk, personnel and physical security must be evaluated in combination with cybersecurity.

Physical security refers to protections against unauthorized in-person access to the physical process and the process control system. Although often

overlooked, numerous industry events have shown that poor physical security can increase the likelihood of both internal intentional attacks (e.g., disgruntled employee) and unintentional incidents (e.g., mistake, accessing incorrect part of system). Physical security is largely outside the scope of this guideline, but it is important for process sites to implement the three key aspects of physical security:

- Access control (e.g., fences, locked gates, access control cards)
- Surveillance (e.g., security cameras, security guards, 24/7 occupancy of control room)
- Policies and procedures (e.g., guidelines for physical security, audits of locked buildings/rooms)

Additional information on physical security can be found in the IEC 62443-2-1 standard [12] as well as in sector specific standards (e.g., CFATS [14], API 1164 Pipeline SCADA Security [24]).

Personnel security refers to the thoroughness of screening and training plant personnel (e.g., operators, engineers, supervisors) before providing access to critical systems. Personnel security requirements are driven by concerns that an employee may abuse their trust and deliberately cause harm to the company or that an employee may unwittingly cause an accident (e.g., inattention, unqualification, substance abuse). People are often the weak link when designing cybersecurity protections and need to be considered in an effective cybersecurity strategy. Requirements for personnel security often include identity verification, background checks prior to employment or on-site access, terms of use agreements for access to the IT and IACS networks, roles and responsibilities, and awareness training.

Even with trusted personnel, cybersecurity hygiene can still be a major factor in achieving cybersecurity goals. Phishing continues to be a major source of cybersecurity incidents, and the accidental downloading unwanted software when accessing file sharing sites (e.g., equipment information, music, movies) is unfortunately common.

Further discussion of personnel security is outside the scope of this guideline, but information can be found in the best practice and industry standard documents from the lists in Section 1.2.2.

1.6 Organization of the Book

This book will provide information in three main parts:

- Part 1: Introduction, Background, and History of Cybersecurity
  - Purpose of this Book (this chapter)
  - Types of Cyber Activities, Who Engages in Them, and Why (Chapter 2)
  - Types of Risk Receptors/ Targets (Chapter 3)
  - Threat Sources & Types of Attacks (Chapter 4)
  - Who Could Create a Cyber Risk? Insider vs. Outsider Threats (Chapter 5)
  - Cybersecurity Case Histories (Chapter 6)
- Part 2: Integrating Cybersecurity Management into the Process Safety Framework
  - General Model for Understanding Cybersecurity Risk (Chapter 7)
  - Designing a Secure Industrial Automation and Control System (Chapter 8)
  - Hazard Identification and Risk Analysis (Chapter 9)
  - Manage the Risk (Chapter 10)
  - Implementing a Holistic Approach to Safety and Cybersecurity (Chapter 11)
- Part 3: Where Do We Go from Here?
  - A Look at Future Development Opportunities (Chapter 12)
  - Available Resources (Chapter 13)

Part 1 introduces process safety professionals to the many different types of cybersecurity events, threats, and attacks that have the potential to negatively impact the process control system. These serve as the foundation for Part 2, which introduces strategies for integrating cybersecurity management into existing process safety activities to better understand, identify, and manage cybersecurity risk by tailoring existing process safety assessment methodologies to address cybersecurity concerns. Finally, Part 3 covers future development opportunities and supporting resources so that companies in the process industry can become better prepared to adjust to and defend against the continually changing cybersecurity landscape.