ENSURING CYBER SAFETY IN AN EVOLVING THREAT LANDSCAPE

Cyber security is a topic that receives increased attention among tank terminal professionals because of the real risks that security incidents pose to them. Frequent news articles regarding security incidents are making headlines around the world. The threat landscape changes, more cyber-attacks focus on specific people, systems and organisations; CEO fraud is much more common than before and storage spoofing is something that most tank terminals have experienced. Threat actors increasingly focus on industrial automation and control systems, especially safety systems. The threat landscape changes and therefore tank terminals need to ensure that their organisation and their infrastructure is resilient to cyber security incidents.

In earlier *Tank Storage Magazine* articles we focused on various cyber security subjects related to industrial automation and control systems (IACS), based on the expertise of Hudson Cybertec in the tank terminal sector. In a previous article we discussed managing security within a tank terminal organisation using a Cyber Security Management System (CSMS). A key element of a CSMS is information and document management. This is an area which does not always receive the attention it deserves. Information and document management is essential to ensure information is available when needed, not only for daily operations but also to maintain overview and control. Naturally for the daily operations, but also keeping the overview and control, in example for auditing. Information and documentation management ensures that data and document are available for the required length of time based on internal or external requirements.

INFORMATION AND DOCUMENT MANAGEMENT

Information and document management for IACS is the process of classifying data, managing documents, safeguarding information and managing access rights for IACS related information. The management for specific IACS-documents is frequently part of a tank terminal's general records retention and document management system. Not having any information and document management at all means an increased risk for the organisation.

Such a document management system is often based upon specific relevant standards and related best practices. Commonly used is the international cyber security standard framework ISO 27000 for information security. But the ISO 27000 cyber security standards framework does not cover specific IACS requirements adequately. Employees working in IACS-environments tend to have little or no control over their information and documentation.

Tank terminals should employ comprehensive information and document management policies for their IACS. Almost all IACS related information is important, often sensitive, and needs to be appropriately controlled and managed. This information must be protected and verified to ensure that the appropriate versions are retained. This requires an information classification system defining the appropriate level of protection.

LIFECYCLE MANAGEMENT

The way any given information asset is managed is determined by its classification level. IACS asset owners are the ones that manage their IACS data and information, even if the data and information is stored outside their immediate or direct control. A lifecycle document management process must be developed and maintained for managing IACS data and information and must establish data entry methods, protection, classification, availability and usability of the IACS information assets. This must be supported by the appropriate policies and procedures.

CLASSIFICATION

Tank terminals must establish classification levels in order to classify all data and information. The classification levels define the appropriate level of protection and its supporting practices, these should address the copying, transmission, sharing and distribution of information. The level of protection must reflect the sensitivity of the information and potential consequences of releasing the information to a wider audience. Some examples of classification levels are; public, restricted and confidential, but any classification can be created.

All IACS information assets must be classified after the classification levels are established. These assets can include control system design information, vulnerability assessments, network diagrams and industrial operation control programmes. Classifying the IACS information assets will indicate the level of protection that needs to be applied.

SAFEGUARDING INFORMATION

The asset owner or responsible individual for any piece of IACS information should ensure that the data and information is safeguarded using appropriate policies and procedures. These policies and procedures are selected based on a combination of multiple factors such as classification level, retention requirements, legal and regulatory requirements, etc. Existing general IT policies and procedures in general do not consider these specific IACS requirements.

Specific IACS requirements might include converting the data to a newer format and/or retaining older equipment that can read the data for long term record retrieval. Other policies might include regular backups and backup testing to verify that these backups can be used for restoration.

CONTROL

Information and document access need to be covered in policies and procedures and the organisation needs to implement access control procedures within the tank terminal. Especially for IACS related data and information access, control must be managed based upon the classification level. It is important to consider that document management systems are traditionally located in IT-environments (outside the IACS environment). In order to maintain control over the IACS data and information contained in an IT-environment, responsibilities must be defined and documented.

POLICIES AND PROCEDURES

The information and document/media management processes must be supported by appropriate policies and procedures. These must include sections for retention, protection, destruction and disposal of information (including written and electronic records, equipment and other media containing information). This must be done to conform to any applicable legal or regulatory requirements. Documents that require retention must document their retention period.

The policies and procedures developed for the IACS information and document management should be in line with and feed into any corporate information and document management system. Legal reviews of the retention policies should be performed to ensure compliance with any applicable laws or regulations.

PERIODIC REVIEW

Hudson Cybertec recommends performing a periodic review or audit of all information and documentation's classification levels. Special control or handling of information or documents must be evaluated during these reviews to determine whether the special control or handling is still required or needs to be changed. A process to increase or decrease the classification level of (a piece of) information or document must also be developed and documented.

A periodic review of the information and document management system itself should also be considered. This ensures that the owners or administrators of the information or documentation still comply to the appropriate policies, standards or other requirements set down by the organisation.

AVAILABILITY OF INFORMATION

Relevant information must be quickly and easily available when needed. In most cases a combination of analog and digital information should be available on a multitude of locations. High quality indexation and search functions allow operators to find the documents rapidly and with ease. Assigned classification levels and any other applicable access rules can be automatically managed, including the proper safeguarding of the information and documentation.

RISKS AND VULNERABILITIES

Based on the tank terminal's vision and goals, a risk-based approach to set up a Risk and Vulnerability Assessment (RVA) is necessary. From the perspective of information and document management, particular risks and vulnerabilities are to be added into the RVA. The RVA itself is one of the first steps and most evident part of a CSMS. Not having any information and document management at all means maximum risk for the tank terminal.

CYBER SECURITY MANAGEMENT SYSTEM

Based on industry best practices the international cyber security standard IEC 62443 specifically provides guidance to manage cyber security within an IACS-environment using a CSMS. The implementation of a CSMS helps tank terminals manage, integrate and maintain cyber security within their organisation and comply with current and future laws or regulations. Information and document management is a key element of any CSMS and is an essential part of the IEC 62443.

The implementation of a CSMS is not a one-off exercise and it will take time to implement within the tank terminal facility and will depends on the size of the organisation. Tank terminals can incorporate existing cyber security controls for the IT-environment into the CSMS. As such, cyber security should be considered as part of existing processes, HSE measures, policies and procedures etc. Once a CSMS has been established it needs to be maintained in order to stay effective.

The tank terminal's vision and goals is the starting point for a CSMS. An effective implementation determines the right balance of cyber security measures that address the three pillars of cyber security: people, process and technology. The security measures are often based upon the results of one or more RVA. The RVA itself is one of the first and critical steps of a CSMS. All information and documentation regarding the CSMS shall be stored and maintained within an information and document management system.

To ensure the success of the development and implementation of the CSMS, tank terminals can ask for independent guidance and expertise from a subject matter expert. Hudson Cybertec supports tank terminals with guidance and expertise including managing the development and implementation of a CSMS.

FOR MORE INFORMATION

This article was written by Ilya Tillekens, senior consultant at Hudson Cybertec.
www.hudsoncybertec.com/en/tsm