Industrial Cybersecurity Services

Cybersecurity Risk Assessments

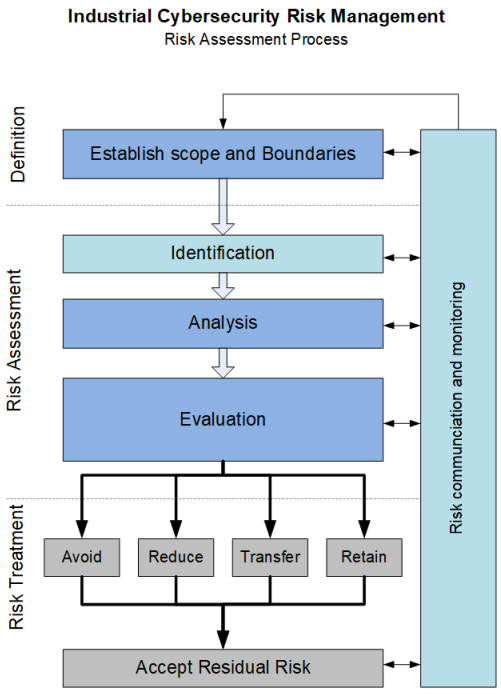
A different approach to risk assessment for industrial computing systems is necessary as these environments tend to be more vulnerable to computing disruption then standard office computing environments. This is due to historical precedence where production systems are changing from the older proprietary, obscure and isolated systems, to the interconnected systems we encounter today. In addition, those production systems are generally changed or upgraded after 10 to 20 years of service, compared to more regular 5-year life spans of office computing equipment. These factors allow for many security vulnerabilities to coexist on industrial systems, making them more prone to cybersecurity threats.

The primary concern of an industrial environment is the necessity to maintain system reliability. The level of securitization (effort and budget) of these systems will depend on several variables, some of which are:

- What is the importance of a system within the facility?
- What will be the impact should the system not function normally or not be available?
- Do these systems run in a stand-alone environment or are they interconnected in a digital network?
- What is the level of risk posed to these systems from cyber-threats (malware, attacks)?
- How well are they protected against human error and misuse?

Industrial automation is increasingly reliant on digital computing systems and devices as these provide a greater degree of flexibility and efficiency. These systems encompass Industrial Control Systems (ICS), Distributed Control Systems (DCS), SCADA Systems, Production Control Systems (PCS) as well as HVAC (heating, ventilation, air conditioning), safety and physical security systems. Most of these systems generally fall outside the operational scope of traditional IT departments and standard security protections. Although there are often overlapping functions and responsibilities, such as those for network management, all other operational plant systems remain under the responsibility of plant operations.

Plant based digital computing systems and devices are heavily relied upon for continuous plant operations; maintaining their functioning reliability (availability and integrity) is thus a risk management prerequisite. It is precisely this degree of reliability that is at the core of the cyber-risk assessment and services.



Human mistakes (unintentional errors) is the primary cause (80% of the cases) of digital computing incidents. It is also these human errors that lead to the increase of potential intentional security incidents through unauthorized access (system hacking). Identifying computing system vulnerabilities, misconfigurations, mobile device usage habits and remote accesses will provide a true picture of security risks. These can then be mitigated by applying proper security measures and strengthening security-based processes to all plant digital computing systems.

A cybersecurity risk assessment will help an industrial site discover unknown vulnerabilities and propose a planning to reduce existing risks.

A risk assessment will primarily cover the following type of services:

- Review the existing site digital computing inventory and infrastructure
- Help determine critical digital computing systems
- Identify technical, procedural and human based security risks
- Provide a set of recommendations to mitigate the identified risks
- Repeatable compliance reviews of security maturity and progress

Copyright