GLOBAL CYBERSECURITY ALLIANCE

Implementing an Industrial Cybersecurity Program for Your Enterprise

THE TIME IS NOW

November 2021

www.isa.org/ISAGCA

Implementing an Industrial Cybersecurity Program

ISA/IEC 62443 provides a powerful tool to reduce the risk of financial, reputational, human, and environmental impact from cyber-attacks on Industrial Automation and Control Systems (IACS). However, since it is a "horizontal standard", 62443 is meant to address a wide range of industries, and any specific company is likely to find that while most of the standard applies to their IACS, parts of it may not. For example, some "normative requirements" that are appropriate for an interstate pipeline, may not be relevant to a chemical plant or a discrete manufacturing facility. There are also obvious differences between a large-scale corporation with many sites and thousands of employees, and a small company with a few dozen staff.

It is therefore recommended that each company establishes their own Industrial Automation and Control Systems (IACS) Cybersecurity Program to manage these cybersecurity risks. ISA/IEC 62443 2-1 provides guidance on how to establish a Security Program for IACS asset owners. This process might look like the following.

This white paper is intended to address the needs of Owner/Operators of industrial facilities. It will discuss the following:

1. What is an IACS Cybersecurity Program?
2. Preparing an IACS Cybersecurity Program
3. How does an IACS Cybersecurity program relate to IT Cybersecurity?
4. Costs and Benefits of an IACS Cybersecurity Program
5. What to do next

In the coming months, ISA plan to publish additional white papers intended for IACS vendors, suppliers of IACS products and services, Integration/engineering services, and possibly other major stakeholders such as insurers and regulators.

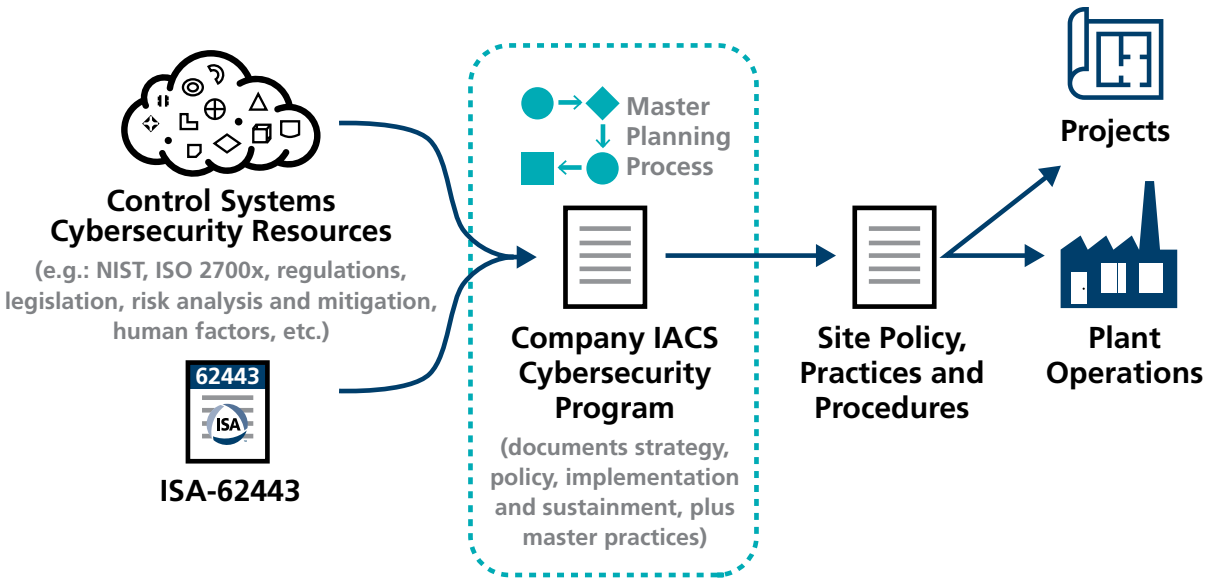

Figure 1. IACS Cybersecurity Program Workflow

What is an IACS Cybersecurity Program?

An IACS Cybersecurity Program (yellow) defines the company's IACS security policies, practices, and procedures associated with the operation and design of the company's industrial facilities.

As this diagram indicates, the ISA/IEC 62443 standard provides Concepts, Practices, and Requirements that may be included in a corporate IACS cybersecurity program.

Note that a Corporate IACS Cybersecurity program is a necessary first step, however, the Policies, Procedures and Requirements defined in this program, must then be implemented within existing Corporate and Facility procedures if they are to be effective. This implementation should be undertaken as one or more projects, with stated schedules, scopes, and budgets; and must include training and management of change to address human and organizational aspects.

At present, the 62443 standard identifies over 550 separate requirements that may be necessary for a given company's facilities. It is impractical to search through ISA/IEC 62443 to determine what is necessary for a given project or operating facility. A key objective of the IACS Cybersecurity Program is therefore to establish approved requirements that may then be incorporated in project or facility standards and procedures.

A corporate IACS cybersecurity program must select which ISA 62443 requirements to include for:

- A company's Existing Facilities
- New company projects that involve IACS

A new company project for IACS can include most of the ISA 62443 requirements that address the design and operation of the asset. Existing Facilities will not be redesigned to meet all those requirements because that effort would be cost prohibitive. Therefore, many design requirements will have to be introduced over a longer period of time as major changes occur to Existing Facilities. These Existing Facilities can quickly address the program and operational requirements in ISA 62443.

As shown in Figure 2, requirements and recommendations from other industry, national, and international standards, may also be considered for inclusion in the company's IACS Cybersecurity Program. Examples of these might include:

- ISA standards such as:
  - ISA84 (safety instrumented systems),

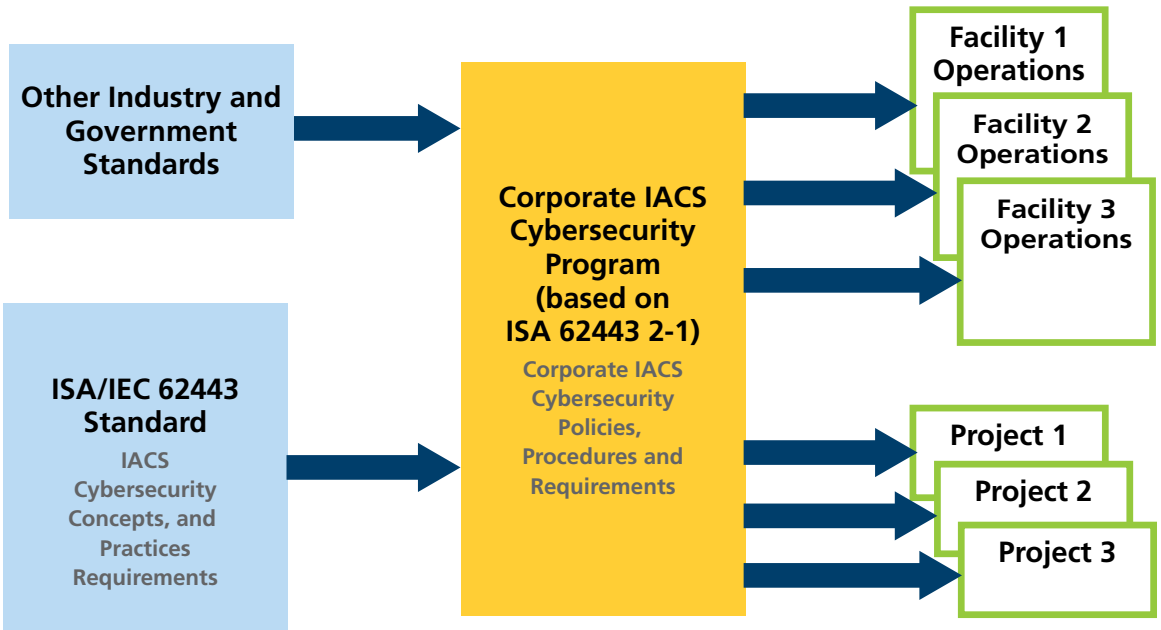

Figure 2. IACS Cybersecurity Program Concept

- ISA95 (enterprise integration),
- ISA100 (Industrial wireless networks), and
- ISA108 (intelligent device configuration)

Note: Since ISA standards are internally "harmonized", use of these together with ISA/IEC 62443 may save considerable time and effort for the Owner/Operator.

- Additional cybersecurity standards and guidelines from NIST, NAMUR, ISO, IEC, and others
- Standards and guidelines for human factors, risk analysis and risk mitigation.
  - Human Factors:
    - » ISO 6385 Ergonomic principles in the design of work systems
    - » ISO 26800 Ergonomics – General approach
    - » API Human Factors 2005 & 2006
    - » IEC 62879 Human factors and functional safety
  - Risk Analysis/Mitigation:
    - » ISO 27xxx series
    - » NIST 800-30 Guide for Conducting Risk Assessments
    - » NIST CSF

Many of the above have been aligned with ISA/IEC 62443, including cross-reference documents and other white papers.

Examples of government standards include regulations and legislation at national, state, and local levels, like NERC-CIP. These must also be considered when creating the Corporate IACS Cybersecurity Program.

ISA is currently active at US Federal, State, and local government levels, to gain acceptance and standardization of regulations based on ISA/IEC 62443. ISA is also participating in programs to promote use of ISA/IEC 62443 in multiple countries around the world.

Preparing an IACS Cybersecurity Program

A formal planning process is recommended to efficiently accomplish development of an IACS Cybersecurity Program. The corporation may have a standard program planning process in place, or may choose to use an alternative such as the PERA Master Planning process. Either way, the general objectives of the program remain the same.

There are a number of advantages to using the PERA Master Planning process for IACS Cybersecurity Planning along with ISA/IEC 62443.

PERA Master Planning is part of the Purdue Enterprise Reference Architecture (PERA) methodology, which is, in turn, the basis of ISA 95, ISA's Enterprise Integration Standard.

- PERA includes Human aspects at all stages of the Master Planning process (especially in steps 4 thru 12), including creation of a separate training plan (step 13).
- ISA99 has compiled a database of over 550 requirements from 62443 that can help automate the creation of a PERA Master Plan.
- ISA99 and ISAGCA are working with Idaho National Laboratories, US National Institute of Standards, and educators including Idaho State University and Purdue University to develop a "cybersecurity skills inventory" linked to 62443 requirements.
- PERA Master Planning results in a set of projects (step 14) including cost/benefits, schedules, and reviews.

PERA Planning also addresses organizational design, including how to manage both responsibilities and reporting structures. This is particularly important, as the Corporate IT Information Security group normally reports through the IT and Finance (CFO) organizations, while IACS safety and security for Operations and Projects report through Engineering and the Chief Technical Officer (CTO). This IT organization is traditionally supported as corporate overhead,

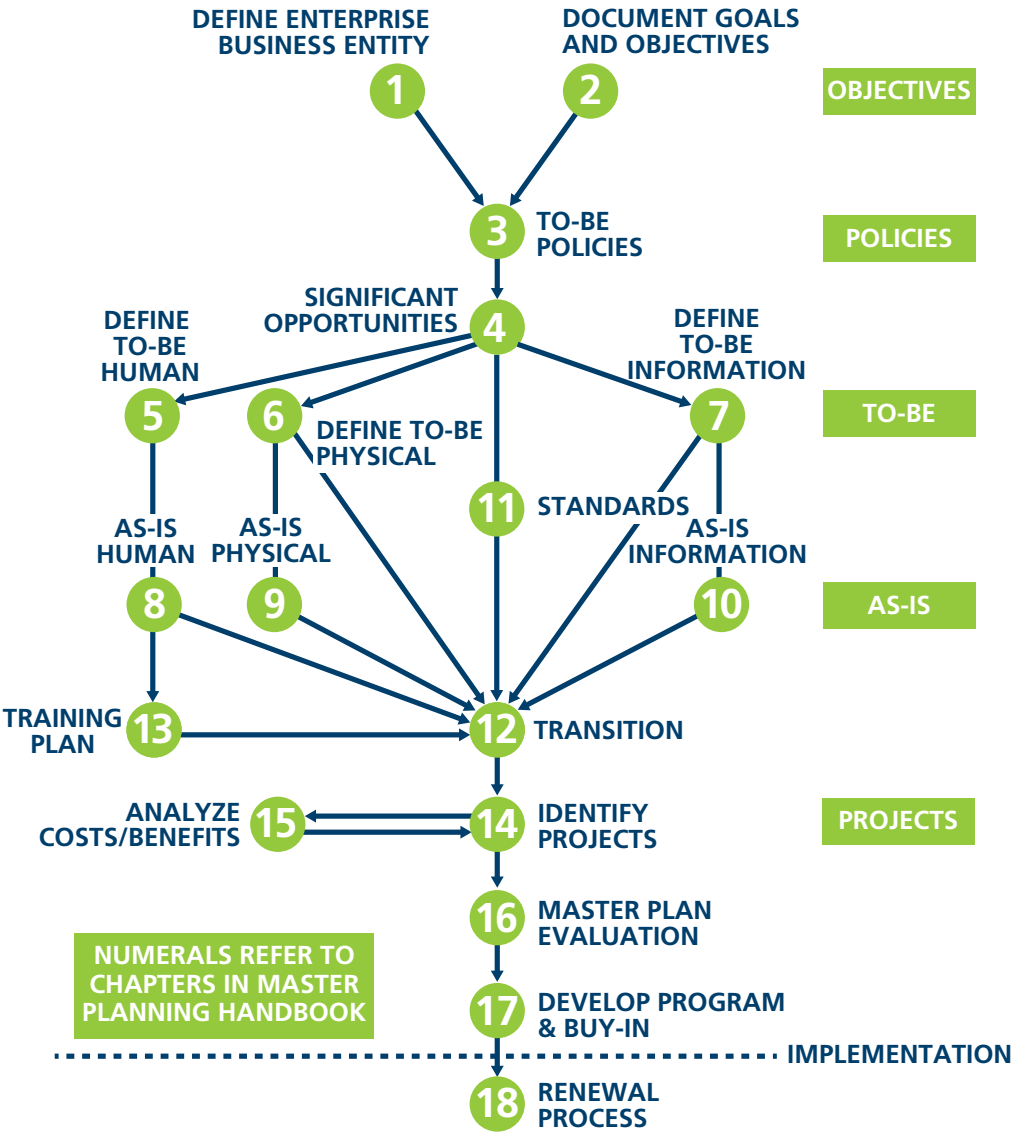

Figure 3. PERA Master Planning Process

including career development, standards, and training. Engineering organizations have traditionally been supported only by projects and operating budgets. If IACS cybersecurity is to be effectively implemented and maintained, a corporately-funded IACS cybersecurity function will be necessary.

Implementing the IACS Cybersecurity Plan

Once the Corporate IACS Cybersecurity Program has been approved (see Step 17 in the PERA Master Planning diagram), the facility may either use the Corporate Program, or, if necessary, create its own facility-specific Cybersecurity Program. In either case, the lifecycle for this IACS Cybersecurity Program will proceed approximately as follows:

a) The first step is an Audit of "As-Is" IACS facilities, including an update of equipment and software inventory, engineering network diagrams and P&IDs (i.e., what is there, and how it is connected). Creation of a list of cybersecurity threats experienced by the corporation and similar industries, is also recommended. ISA99 is assembling a database of threats that can be reported by Industry, Phase, Principal Role, etc., which will be available soon. A whitepaper will be released describing the database and how it can be used.

b) Then, an assessment is made of the threats, vulnerabilities, consequences, and impacts (including the proposed risk mitigation measures), using the assessment methodology described in ISA 62443 3-2. These risks must also be aligned with the corporation's standard risk management procedures and criteria, to allow the company to make investment decisions on a consistent basis.

c) The risks, costs and benefits of the solutions defined in the IACS Cybersecurity Program are compared, including the selected risk mitigation measures (the To-Be State).

d) An As-Is / To-Be Transition Plan is then established, including provisions for financing, staffing, and scheduling of the individual projects, general cybersecurity training of all relevant personnel, and modifying appropriate company policies, practices, and procedures to address requirements defined in the IACS Cybersecurity Program.

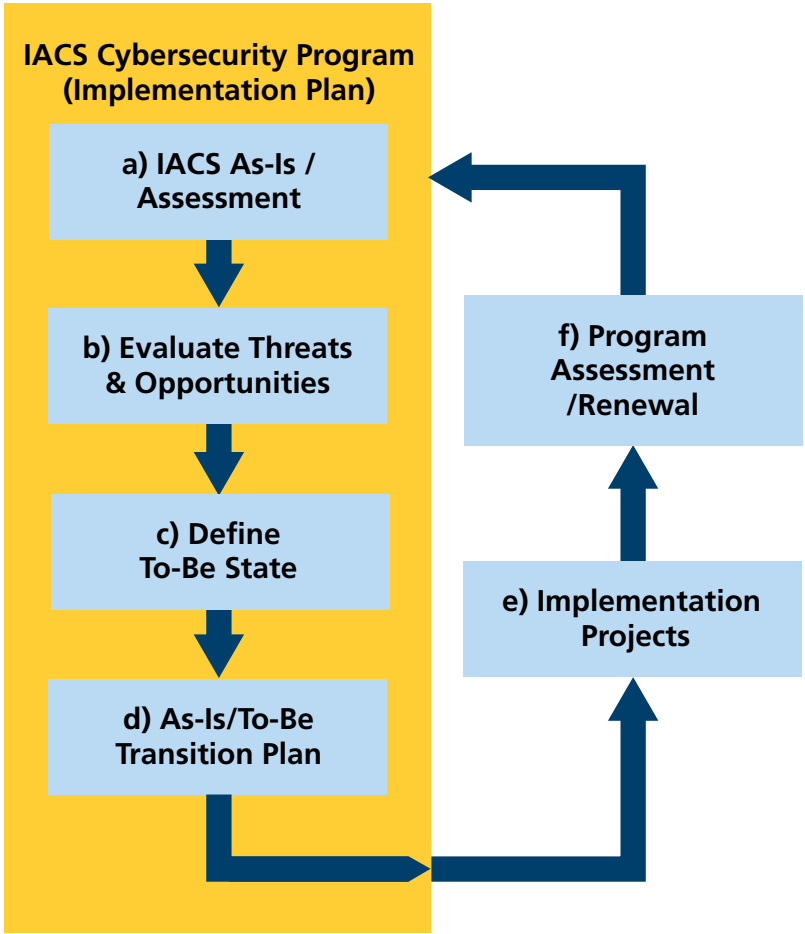

Figure 4. IACS Cybersecurity Program Lifecycle

It may even be appropriate to modify these procedures for different company facilities to address special requirements. Thus, a second level of review/approval could be required at each site.

Until a company has an IACS Cybersecurity Program in place, it may be expedient to implement certain 62443 requirements directly in the company policy, practices, and procedures for a project or site. While this may be unavoidable for new projects or urgent plant situations, it is not recommended as a standard approach. It is likely that important issues will be overlooked, and in any case, the effort required to address a full suite of requirements "piecemeal" is more

expensive than a systematic corporate-wide implementation.

Key Performance Indicators (KPIs) and/or other standard company measurements may be implemented to provide ongoing assessment of the IACS cybersecurity projects. Each IACS Cybersecurity project should be subject to regular review by an external party, and ineffective program elements are eliminated or upgraded.

A periodic audit of the overall IACS Cybersecurity program is also recommended (see Step 18 of the PERA Planning Process). This should include feedback to the corporate IACS Cybersecurity Committee. Changes to the program should be accomplished as part of the company's regular budgeting process.

How does IACS Cybersecurity relate to IT Cybersecurity?

Many corporations already have a corporate position responsible for cybersecurity of information. This position typically resides in the corporate IT (Information Technology) department. The most widely used standards for IT cybersecurity are the ISO 27000 series and selected guidelines from NIST.

Although not yet as common, many corporations are establishing a corporate role that is responsible for OT (Operations Technology) cybersecurity. While IT Cybersecurity is responsible for Information Cybersecurity, OT Cybersecurity is responsible for cybersecurity of IACS. ISA/IEC 62443 is widely accepted as the global standard for IACS cybersecurity, much as ISO 27000 series is for Information Cybersecurity.

Thus, ISA/IEC 62443 and ISO 27000 are, in effect, "parallel" standards, as shown in the diagram below.

The distinction between where ISA/IEC 62443 and ISO 27000 are applied is also indicated in this diagram.

A Corporate IACS Cybersecurity Program (yellow) will contain Requirements for all enterprise phases of corporate facilities including project design phase, and operations phase. These may include project deliverables such as design documentation and drawings (lower right in this

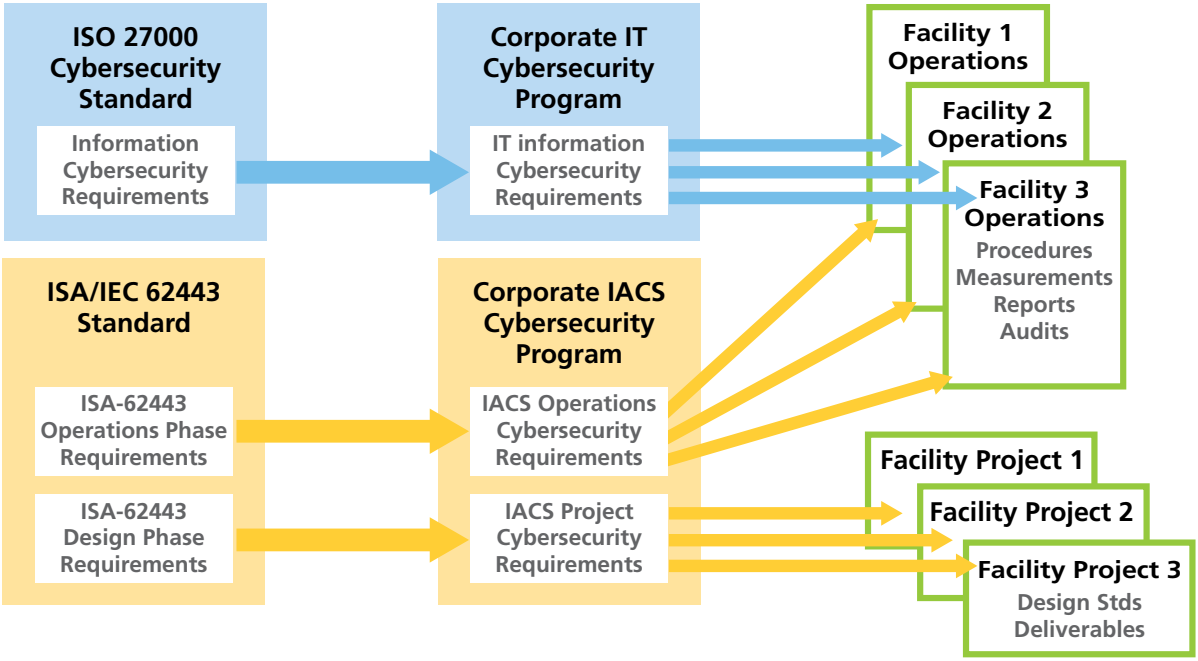

Figure 5. Mapping of Cybersecurity Requirements

diagram), or Operations deliverables such as Operations measurements (e.g., KPIs), incident reports, etc. (upper right in this diagram).

It should be noted that the security of IT information is focused on Operations phase at plants and corporate offices (blue arrows above). Although company information security objectives during project execution may be specified by the Owner, the actual security of information on projects is normally performed by the Integrator, equipment supplier, or engineering contractor.

Typically, information security for IACS in plants (as an addition to operating safety) should be managed by those responsible for the IACS Cybersecurity Program. However, company standards for security of this Information should be provided by the Corporate IT Information security program.

Once areas of responsibility for plant control and automation are agreed in the IACS Cybersecurity Program, the standards to be used for safety and security of IACS systems and related components will be selected and documented (see Step 11 in the PERA Planning Diagram).

Finally, the corporate IACS cybersecurity program, and the corporate IT cybersecurity program, should be aligned, as they provide complementary parts of overall corporate cybersecurity.

Costs and Benefits

An IACS Cybersecurity Program should be assessed and budgeted like any other investment made by the corporation. Implementation of the proposed cybersecurity plan will be divided into a number of projects, each of which is individually justified, approved, and tracked (see Step 14 in the PERA Planning Diagram).

To facilitate this evaluation, cybersecurity risks will be assessed using accepted industry and company criteria. A series of measures will then be evaluated that may mitigate these risks, and the cost of these measures compared to the risk reduction benefits (see Step 15 in the PERA Planning Diagram).

As part of the evaluation of the corporate IACS Cybersecurity Program, there should be a comparison of possible program costs and Health-Safety-Environment (HSE) impacts from IACS security breaches vs. the costs of the proposed IACS Cybersecurity Program. The IACS Cybersecurity Program must effectively manage HSE impacts regardless of program costs. The likely cost of an IACS breach or failure of the IACS Cybersecurity Program is typically much more than for an information breach, since in addition to the risk of data loss, actual physical plant operations may be impacted, and/or loss of production and/or equipment damage.

These costs are in addition to the likely costs of information security breaches or other failures from not having an IACS Cybersecurity Program, including:

- Injuries or death
- Environmental damage
- Long-term loss of operational permits or other government intervention
- Loss of production
- Lawsuits
- Loss of revenue due to reputational or brand damage
- Penalties and fines
- Ransoms and other costs to recovery operations
- Increased insurance premiums

Balanced against the risk of losses are the costs of mitigation measures, including staffing and training of Corporate and Plant Personnel.

Other benefits of the IACS Cybersecurity Program may be realized, including

- More efficient use of staff
- Insurance savings
- KPIs and employee awareness (eg., number of attacks vs penetrations, time from attack to detection)
- Benefits of improved asset tracking and IACS architecture documentation

What to do Next

The number of IACS cyber-attacks, and the financial impact of these attacks, are increasing rapidly. Average losses associated with each attack are reaching tens and even hundreds of millions of dollars, particularly in "infrastructure industries" like power generation and distribution, oil and gas processing, petrochemicals, and pipelines. This is increasing the urgency for corporations to establish IACS Cybersecurity Programs to address these risks.

Using ISA/IEC 62443 and the IACS Cybersecurity planning process, companies can apply their existing Control and Automation expertise, rather than hiring new staff, or training consultants on the operation of their facilities. This is increasingly important, as studies have indicated that over 1.5 million cybersecurity jobs remain unfilled in 2021, and that this is likely to increase in 2022.

It is also true that the risks and costs associated with cyber-attacks on IACS are too high to simply assign technical project and operations personnel to "solve the cybersecurity problem".

The IACS Cybersecurity program should therefore be created and managed by business and technical leadership, via a tiered IACS cybersecurity council. This may include at the first tier, CEO, CTO, COO, CFO, CIO and H/R, as well as at the second tier, senior staff in their organizations who are involved with cybersecurity standards and procedures, such as the CISO (Chief Information Security Officer), and the Corporate Security Manager.

One of these executives should be given the role of "Program Champion". The Chief Technical Officer is a logical choice, as the CTO is responsible for engineering staff who design major projects, and operations staff who operate IACS control systems. The Champion will report progress on the IACS Cybersecurity Program to a review board, that should include major stakeholders including representatives of:

- Plant Operations
- Capital Projects
- IT Operations
- Control and Automation Systems
- Physical Plant Security
- Corporate Risk Management
- Health, Safety and Environmental

The employee evaluation, salary, and reward system at the company should be updated to ensure IACS leaders throughout the company are accountable for deploying and supporting the IACS Cybersecurity Program within their organization. Using ISA/IEC 62443 and PERA Master Planning, expenditures for initial phases of IACS Cybersecurity Program Planning are relatively modest, and can probably be funded from existing standards and training budgets. However, creation of the actual corporate program will likely require several months with a dedicated small team.

It should also be noted that the personnel required for an IACS Cybersecurity Program Plan should largely be drawn from existing enterprise resources. It is not possible to create an effective IACS Cybersecurity Program without engineers and technicians who have a deep understanding of the corporation's industrial facilities, IACS, industrial networks, hazards, and organization. Thus, even if "cyber-certified" engineers and specialists were available, the cost to train these new hires or consultants would be excessive, and in any case, would delay implementation of an effective IACS cybersecurity program by many months or years.

The best approach is therefore to support and encourage professional development of current staff, including IACS cybersecurity training and certifications. This may be accomplished in parallel with creation of the IACS Cybersecurity Plan and implementation of the resulting Corporate IACS Cybersecurity Program.

If you would like more information on the above, please contact

Gary Rathwell, President
Enterprise Consultants International Ltd (ECI)
Gary.Rathwell@Entercon.biz, or
Gary.Rathwell@PERA.net

ISAGCA Member Companies

1898 & Co. (Burns McDonnell)
ACET Solutions
aeSolutions
BaseRock IT Solutions
Bayshore
Carrier Global
Claroty
ConsoleWorks
Coontec
CyberOwl
CyPhy Defense
Deloitte
Digital Immunity
Dragos
Eaton
exida
Ford Motor Company
Fortinet
Fortress InfoSec
Honeywell
Idaho National Laboratory
Idaho State University
ISASecure
Johns Manville
Johnson Controls
KPMG
LOGIIC
Mission Secure
MT4 senhasegura
Munio Security
Nova Systems
Nozomi Networks
PAS
PETRONAS
Pfizer
Purdue University
Radiflow
Redacted
Red Trident
Rockwell Automation
Schneider Electric
Surge Engineering
TDI Technologies
Tenable
TI Safe
Tripwire
TXOne Networks
UL
Wallix
WisePlant
Xage Security
Xylem

Join the Movement: Contact ISA to Learn More

Let's talk about how your company or organization can join us—contact **Rick Zabel** at rzabel@isa.org or +1 919 990 9233.

Press and media should contact ISA's Director of Marketing and Communications, **Jennifer Halsey**, at jhalsey@isa.org or +1 919 990 9287.