WHITE PAPER

Securing industrial systems in a digital world

Approach cyber security with confidence

Securing industrial systems in a digital world

Approach cyber security with confidence

The state of industrial cyber security

The development of Industrial Control Systems (ICS) over the past two decades has changed the face of many industries. Operational Technology (OT) – largely industrial equipment – has become increasingly connected, and the integration of Information Technology (IT) components allows such devices to leverage software that drives data collection and analysis, resulting in enhanced performance and ultimately "smarter" machines.

With these benefits came vulnerabilities, including the possibility of malicious actors gaining access to critical assets through networks. The growing recognition of cyber security threats to critical infrastructure (e.g. energy, water, transportation) has brought the topic into the spotlight. Further, regulatory requirements on these industries have increased. Standards and policies have been created in an attempt to address the rapid technological changes; however, it is still challenging for companies to implement needed processes and keep personnel up to date and aligned, given the pace of change.

Meanwhile, the cyber threat landscape continues to increase. According to IBM, the number of attacks aimed at ICS increased by 110% in 2016 compared to 2015.[1] To add to this, leveraging third-party vendors and new cloud-based services result in additional areas of risk previously non-existent in ICS.

Designing products to be secured from cyber attack only became a topic of concern about a decade ago, and the prevailing sense at that time was that isolation ("air gap") and limited availability of technical knowledge ("security by obscurity") protected ICS products. This false belief was quickly dismissed as wishful thinking after Stuxnet (see next page), and vendors began to respond to customer demands for more secure products. However, with often heterogeneous equipment and life cycles counted in decades, it will take time for secure components to become the norm.

In this paper, we will share insights to enhance your understanding of the ways in which governance, technology, and business requirements intersect. We will also illustrate ways in which organizations can leverage digitalization opportunities to better manage increasing risks. We will break down these risks to help your organization address these sometimes overwhelming challenges. Further, we offer recommendations for organizations to improve their cyber security posture in a holistic and sustainable model.

[1] https://www.securityweek.com/ibm-reports-significant-increase-ics-attacks

The impact of real cyber attacks

These events offer an overview of the history of cyber attacks on ICS and help give a clearer picture of the potential negative impacts of weak cyber security.

2010 Stuxnet

- First publicly-known example of a cyber weapon
- Designed to disrupt the Iranian nuclear development program
- A self-propagating application (a “worm”) spread via USB drives and network connections
- It took over the PLC controlling the uranium enrichment centrifuges and ultimately caused these to break down at an accelerated rate
- It was able to operate undetected for an extended period of time

2014 German Steel Mill

- Second confirmed case of a cyber attack causing physical damage
- Attackers used a spearphishing campaign to capture user credentials
- They connected through the business systems to the OT network
- Caused massive damage when a blast furnace had to be shut down abnormally

2014 Havex/ Dragonfly

- Victims from multiple industries, including energy, manufacturing and pharmaceuticals
- Malware campaign using multiple attack vectors
- These were spearphishing, waterhole poisoning, and replacing suppliers’ support websites
- Installed a Remote Access Trojan (RAT) on systems inside targets’ networks
- RATs coordinated and updated via the internet

2015 and 2016 Ukraine Power Grid

- Blackouts to parts of the Ukrainian grid in December 2015 and 2016
- In 2015 approximately 30 substations were shut down
- The attackers infiltrated production SCADA networks of 3 power companies
- Workstations and servers were infected with malware
- Reconnaissance carried out over an extended period of time
- Other actions further disrupted restoration efforts
- The 2016 incident utilized an automatable tool; reconnaissance activities carried out independently
- Analysis showed that its full capabilities were not used

2017 WannaCry

- Ransomware attack that impacted Windows servers, specifically around vulnerabilities in system updates
- Requested Bitcoin payment from victims
- Parts of the UK's NHS were infected, as well as Spain's Telefónica, FedEx and Deutsche Bahn
- It was a known vulnerability that could have been solved with patch management

Prevention was possible in all of these cases if proper security controls were in place.

Meeting cyber security challenges

Companies operating ICS face a number of challenges due to the developments and risk outlined previously.

Regulatory requirements

In an effort to address cyber security risks, the number of regulations and standards that have been created by governments, industry groups and private organizations has grown considerably over the past 10 years (some examples follow in the Governance section below). Organizations must go through the effort of understanding the regulatory environment, determine which regulatory requirements are applicable to them, and then continuously monitor for updates and changes to regulation to confirm compliance with the latest versions. Additionally there is a very real threat that even when an organization attempts to faithfully comply, a lapse in proper execution can expose them to potential fines.

Although necessary, meeting regulatory requirements, and the endless focus on compliance, plus the reporting and documentation that this entails, can consequently be both daunting and taxing. Nevertheless, this is necessary because in many cases, compliance is a precursor to doing business with customers. It's considered a way to show that the minimum cyber security requirements have been met.

In reality, compliance is a byproduct of security. Organizations need to look at security from a holistic standpoint, not a 'check-the-box' or bare-minimum compliance standpoint.

Recommendations for how to approach security more comprehensively follow in the sections below.

Workforce shortages

The three foundations of cyber security are people, process, and technology. While many organizations' policies focus on the latter two factors, it should be noted that people are just as critical to maintain a robust security posture.

The tremendous changes in technology are now resulting in increased demand for new skills and skill combinations; the current demand for cyber professionals is not being met. Cost pressures and workforce reductions only compound this situation and can result in documentation slipping through the cracks and, ultimately, in a lack of compliance with regulatory requirements, as mentioned above.

Recommendations: Many companies address this shortfall by building collaborative teams drawn from both IT and OT staff within the organization. Other organizations turn to third party providers to deliver IT/OT expertise that is shared among multiple customers through managed services. Automation of routine security maintenance tasks and reporting can significantly reduce this burden as well. For more info: ABB Collaborative Operations Centers

A positive effect is that retraining programs and a greater interest in the cyber security space from a professional education perspective are becoming increasingly common.

Some of the major cyber security training programs and certifications are:

- **SANS Institute** – largest provider of cyber security training, side focus of preparing people for cyber security certifications and other widely recognized programs in the industry
- **CISSP** – Certified Information System Security Professional, considered a rite of passage for CISO (Chief Information Security Officer) professionals
- **GICSP** – Global Industrial Cyber Security Professional, the equivalent certification recognized within industry

Cyber asset inventory

It is not always a given that organizations have a full inventory or visibility of all the components across their operational enterprise, or in their ICS or those of third party service providers. This can have a negative effect in the case of a vulnerability, as an organization tries to understand the impact and react accordingly. Where a cyber asset management system is not already in place, manual effort is required, resulting in increased costs and lengthy reaction times.

It is a case of: "You can't measure what you don't know"
Peter Drucker

Recommendations: When installing new equipment or systems, organizations should also install programs that real time present a report of their asset inventory (i.e. number of servers, HMIs, etc.). Such a system also allows users to look up multiple versions of products to determine their susceptibility to vulnerabilities.

The greatest challenge during incident response is the triage process. Asset inventory solutions take the triage process from being a manual effort to being automated, thereby shortening reaction times and reducing costs.
For more info: ABB Cyber Security Monitoring Service

Life cycle of products

As mentioned, historically ICS systems were not designed with cyber security as a first priority. While organizations may have more opportunity to implement cyber security standards in new products and systems, for older ICS it can be more difficult. This difficulty notwithstanding, organizations are still expected to address the cyber security needs of these previously installed systems which are likely to have many fewer support options.

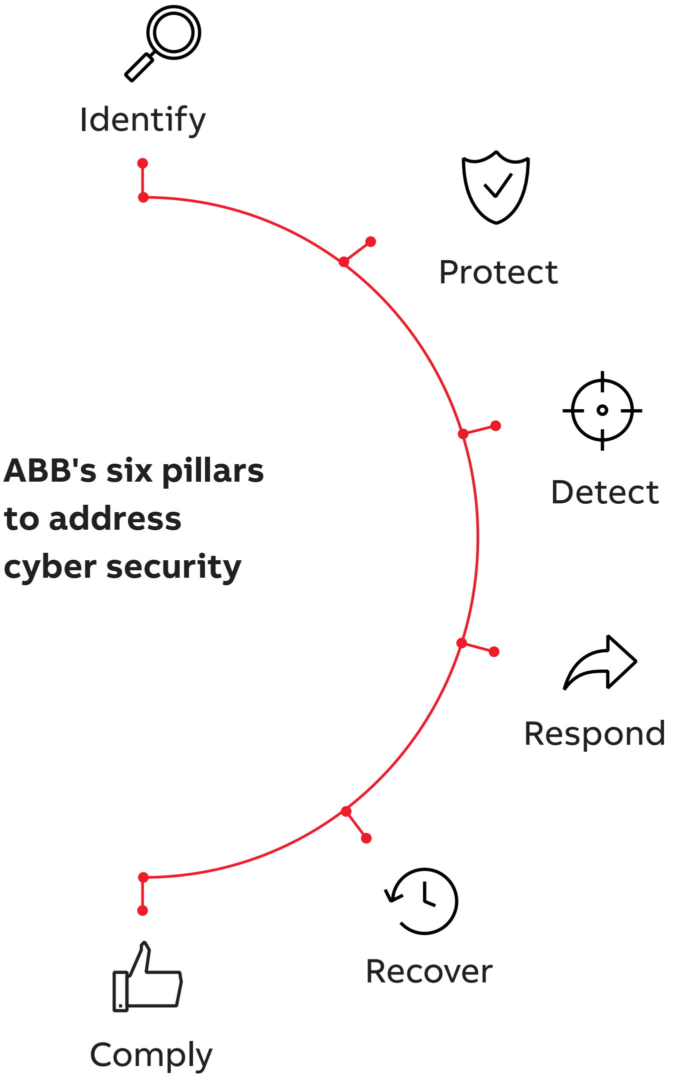
This means that remediation needs for older ICS are at times unknown to the organization, and when known can be challenging and costly. In addition, many product life cycles are counted in decades, rather than years, and it is not always straightforward to find capital to replace or upgrade products quickly.

Recommendations: Together with ICS system providers, organizations should evaluate their existing operations base and prioritize remediation. A risk assessment will highlight what is worth fixing immediately. Organizations can prioritize and still greatly impact their risk posture.

Moving forward, organizations need to ensure that their programs and systems are secure by design and secure by default so that they do not have the same challenges in the next generation of products.

How to implement baseline security measures for every ICS organization

In addition to addressing these challenges, here are some recommendations for ways to address cyber security at each pillar of the cyber security life cycle. ABB uses six pillars to address cyber security.



ABB's six pillars to address cyber security

Ability to Identify

Executive Support

An organization should establish a comprehensive security program with the support of the executive team. Executive leadership determines the budget for the overall company based on its level of risk tolerance; a strong cyber security program will require a significant investment, and large budgets are awarded aligned to organizational priorities. Executive leadership also has the authority to encourage and enforce that employees follow new cyber security procedures, as opposed to ad-hoc uncoordinated security. Before beginning to put measures in place, it is therefore essential to align the program to corporate risk appetites and to obtain executive support of the roadmap.

Cyber Security Audit

Very few companies have complete, up-to-date and documented records of their entire networked systems and assets. The concept of a cyber security audit is not new, but has been uncommon for ICS. However, due to the challenges companies have had to keep documentation current, they are an appropriate place to start. External or third party audits can be a useful tool to drive companies to do a better job at maintaining an up-to-date inventory of all hardware and software. This includes documenting configurations, mapping networks, and identifying vulnerabilities and exposures. This information is essential to risk management.

Ability to Protect

Harden all Hardware and Software Configurations

Systems and devices usually do not ship configured for maximum security but for ease of use and access. Ports and services which may not be called for in the actual workplace environment may be left open by default. Hardening these assets, for example turning off software features and functions or enabling key access requirements on devices, reduces risk by decreasing the number of ways a malicious actor can attack them.

User Accounts and Least-Privilege

As ICS environments become more reliant on connected computers for operational purposes, it is important to manage and apply user permissions and security policies across the entire ICS environment. Using a domain server with Active Directory or LDAP (Lightweight Directory Access Protocol) can help push consistent security policies to all your user machines. User permissions can be assigned to specific roles to ensure every user has the least number of privileges allowable for executing their job. Security policies and user permissions are powerful tools to enforce best practices for things such as password policy, file access, removable media, etc.

Integrated Update and Patch Management Program

Applying software updates and patches often receives low priority until an incident actually occurs. There are undoubtedly challenges to patching, including compatibility questions, uptime requirements, and manufacturer warranty constraints, and in some cases these may prohibit updates entirely. An update and patch management program allows an organization to evaluate the risks in installing, delaying, or not installing patches and to determine its best plan of action, which may involve adding layers of other security controls around unpatched systems. Tools to automate the back-up and patching of systems can significantly reduce the labor burden and cost of applying patches.

Network Segmentation

Due to the growth of digitalization, many companies have embraced new connectivity at a rapid pace, unintentionally leaving networks with unprotected or inadequately protected points of access. Segmentation is key to reducing the impact of security breaches by adding control points and inhibiting the spread of malware. While companies have made efforts to segment their network, this has not always been achieved with optimally secure results. The outcome is that companies think they have segmented networks, but in reality they have a flat architecture which opens up more risk. Organizations are encouraged to review network diagrams on a periodic basis to ensure the network in place matches what has been documented.

Ability to Detect

Continuous Vulnerability Assessment and Remediation
Vulnerabilities in networked systems are discovered frequently, and it is the responsibility of the organization to become aware of these as soon as possible. Actively monitoring sources such as ICS-CERT, vendor websites, and industry journals is a best practice for an organization to increase awareness. A more proactive approach is to subscribe to receive push notifications which are specifically related to a system's installed components. Product and system suppliers must provide options for customers or any affiliate to confidentially report a security concern to promote timely remediation.

Intrusion Detection and Prevention
It is becoming increasingly important to monitor ICS-specific protocols and define the anomalies to normal operations. With this monitoring comes the need for log collection, aggregation and analysis. Because the ICS industry is production focused, there are challenges with trusting IPS (Intrusion Prevention System) active blocking policies that may interrupt operations. There are however a number of passive monitoring technologies which can help identify a potential threat without adding to the risk of disruption. As the industry becomes comfortable with the analysis of these cyber security anomalies, and more readily allows implementation of active prevention policies, additional protection from cyber threats to the ICS environment will be possible.

Ability to Respond

Incident Response
It is highly likely that all organizations will eventually experience a security incident. The impact of that event is largely determined by the strength of a company's incident response program. Thoroughly planning and communicating what actions are to be taken by each party ensures a coordinated response and greatly reduces the potential negative impact. Having a strong communication plan, with already drafted holding statements, in place helps customers and all those impacted feel more comfortable in the case of an incident. Holding incident response exercises allows companies to practice and gain familiarity with roles and responsibilities.

Ability to Recover

Back-up and Restoration Plans
Organizations must be able to back up and restore their systems to a near real-time position regardless whether the event was caused by a cyber attack, human error or physical failures. Unfortunately some organizations find out that proper back-up and recovery plans do not exist only after the event has occurred. This will greatly reduce the speed of recovery which will increase the overall negative impact of the event. Ensuring that networking devices, HMIs, controller configurations, and PLC configurations are backed up on a regular basis is imperative to a quick recovery. A planned and tested recovery strategy is key to reducing the impact that a cyber attack may have on your environment. Tools that can automate back-up can also reduce the burden of performing routine back-ups to employees.

Ability to Comply

Security Training Programs
Security is a product of people, process, and technology, and organizations often forget that these people include every individual with access to their networks and assets. Security awareness training of all personnel is a necessity to not only educate everyone on their role but also to change corporate culture to one which prioritizes a robust security posture. See the Workforce Shortages section above for more information on specific training programs and certifications.

Effective risk management

Risk can be broken down into two categories: operational risk and cyber risk. In terms of operational risk, the effects tend to be more tangible including equipment failure, personnel safety, or environmental impact. In contrast, the goal for cyber risk is to manage an organization's exposure to vulnerabilities that may cause data loss, privacy concerns, or reduced network security. Ultimately, uptime, efficiency, revenue loss, and reputational damage are key focus areas regardless of type of risk.

The challenges outlined above, for example cyber asset management, increasing industry standards, cost pressures and staff reductions, make measuring cyber risk difficult. This section will focus on best practices to achieve this goal.

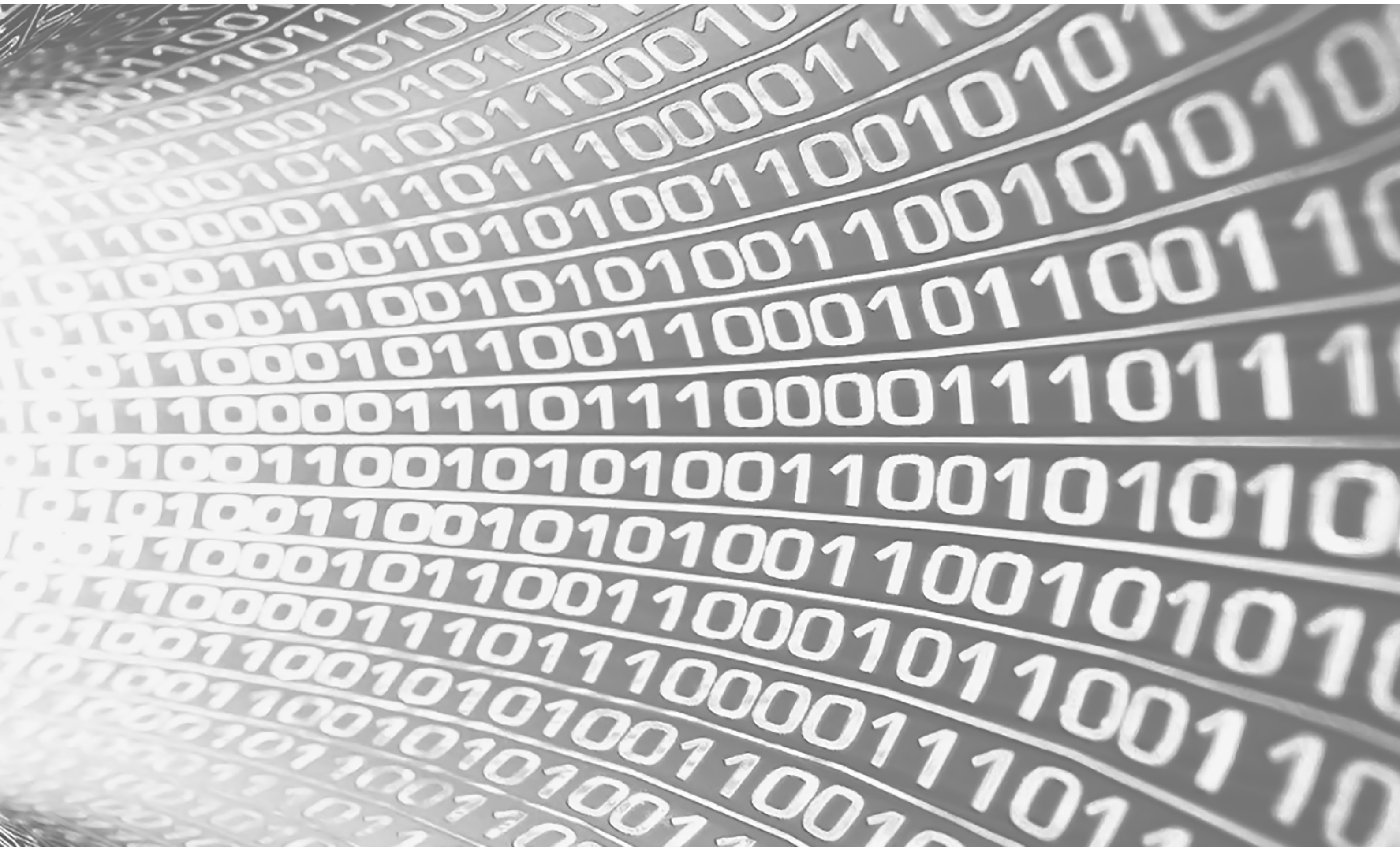
Best practices to measure cyber risk

1. Choose a consistent method to quantify cyber security risk. In theory, this is simple but in reality it is more challenging. The method must be adjusted to align to a company's unique use case.

2. The holistic organization (not only IT/OT/Technology) should set the risk thresholds and obtain acknowledgement from the organization at large. The risk threshold must be easy to understand. For example, a threshold must explicitly define what is acceptable versus not acceptable as opposed to measuring risk on a scale of 1-5. It is critical to make measurement easy to comprehend for all.

3. Align the cyber risk to enterprise risk. Risk has been traditionally presented to company executives and the board collectively. Boards are evaluated on measuring risk in an organization and are personally liable for decisions made. A main reason cyber risk management seems more complicated than it might be is because of the distinction in how risk rolls up to management.

4. Security is a continuous effort. Organizations should strive for increased cyber risk management maturity levels each quarter, year, and period.



Cyber security information sharing

Information sharing is one of the key activities organizations can engage in so as to optimize their efforts in meeting cyber security challenges. The aim of the following organizations is to coordinate efforts between government and industry, in some cases across multiple sectors, allowing information, knowledge and expertise to be shared. An organization should select information sharing groups to stay up to date on what may be relevant to their given industry or company.

ICS-CERT	The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), part of the Department of Homeland Security, works to reduce risks within and across all critical infrastructure sectors by partnering with law enforcement agencies and the intelligence community and coordinating efforts among Federal, state, local, and tribal governments and control systems owners, operators, and vendors. Additionally, ICS-CERT collaborates with international and private sector Computer Emergency Response Teams (CERTs) to share control systems-related security incidents and mitigation measures. For more info: https://ics-cert.us-cert.gov/
ICSJWG	ICS-CERT established the Industrial Control Systems Joint Working Group (ICSJWG) to enable communication and partnering across all Critical Infrastructure Sectors between private industrial control system owners/operators as well as national agencies and departments. ICSJWG holds twice-yearly conferences and publishes newsletters and webinars on ICS security subjects. For more info: https://ics-cert.us-cert.gov/Industrial-Control-Systems-Joint-Working-Group-ICSJWG
National Council of ISACs	Sector-based Information Sharing and Analysis Centers (ISACs) collaborate with each other via the National Council of ISACs. Formed in 2003, the NCI today comprises 24 organizations. It is a coordinating body designed to maximize information flow across the private sector critical infrastructures and with government. ISACs collect, analyze and disseminate actionable threat information to their members and provide members with tools to mitigate risks and enhance resiliency. ISACs reach deep into their sectors, communicating critical information far and wide and maintaining sector-wide situational awareness. ISACs most likely relevant to your organization include Electricity ISAC (E-ISAC), Emergency Management and Response ISAC (EMR-ISAC), Industrial Control Systems ISAC (ICS-ISAC), Supply Chain ISAC (SC ISAC), and Water ISAC (WaterISAC). For more info: https://www.nationalisacs.org/
EuroSCSIE	The European SCADA and Control Systems Information Exchange (EuroSCSIE) consists of members of European governments, industry and research institutions that are dependent upon and/or responsible for improving the security of industrial control systems. It enables members to share ICS/SCADA security-relevant information. For more info: https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services
ERNCIP	The European Reference Network for Critical Infrastructure Protection (ERNCIP), established under the European Commission's Joint Research Centre, provides a framework for experimental facilities and laboratories to share knowledge and expertise in order to standardize test protocols throughout Europe. This results in better protection of critical infrastructures against all types of threats and hazards and establishes a single market for ICS security solutions. The ERNCIP publishes research papers in addition to standards, best practices and guidelines. For more info: https://erncip-project.jrc.ec.europa.eu/
AISA	As a nationally recognized not-for-profit organization and charity, the Australian Information Security Association (AISA) champions the development of a robust information security sector by building the capacity of professionals in Australia and advancing the cyber security and safety of the Australian public as well as businesses and governments in Australia. Established in 1999, AISA has become the recognized authority on information security in Australia with a membership of over 3,000 individuals across the country. AISA caters to all domains of the information security industry with a particular focus on sharing expertise from the field at meetings, focus groups and networking opportunities around Australia. For more info: https://www.aisa.org.au/

Cyber security governance

There are a number of standards, regulations and guidance documents available, developed by one or more corporations, associations, regulatory bodies or standards organizations, and which may be voluntary or mandatory. Such works, for example, support compliance, improve risk management and outline recommended procedures as related to cyber security. It is important to know which ones are mandatory and/or advisable for your organization. Our recommendation is for organizations to leverage this information to best fit their business model. Some of the most widely recognized are outlined below.

Name	Summary	Country	Industry
NERC CIP	The North American Energy Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Reliability Standards require compliance with all bulk power system owners, operators, and users in North America. These Industry Standards are made mandatory by the authority of the Federal Energy Regulatory Commission (FERC) and Canadian government agencies. NERC has a range of actions available to address non-compliance, up to and including sanctions and financial penalties, but prefers to address and mitigate issues rather than penalize, and to this end does offer some compliance training. There are numerous Standards and many resources are available to help plan and evaluate an entity's compliance, the most important of these being NERC's own site. For more info: http://www.nerc.com/Pages/default.aspx	United States	Utility
Bioterrorism Act of 2002 (PL 107-188)	This Act mandates that all public water systems in the US serving 3,300 or more: • Perform a vulnerability assessment and submit this to the Environmental Protection Agency. • Establish an emergency response plan informed by the findings of the vulnerability assessment and submit a letter verifying this to the EPA. For more info: https://www.awwa.org/legislation-regulation/issues/utility-security.aspx	United States	Water and Wastewater
NIST Cybersecurity Framework	The National Institute of Standards and Technology, a non-regulatory entity within the US government, publishes the non-mandatory guidance on cyber security policy titled the NIST Cybersecurity Framework (NIST CSF). While developed to improve cyber security risk management of US Critical Infrastructure, it has been adopted by many other organizations as well. The CSF is widely acknowledged as thorough but considered by some to be excessive for smaller organizations. As of the NIST Small Business Cybersecurity Act of 2017[2] and the MAIN STREET Cybersecurity Act of 2017[3], NIST has been charged with considering small businesses in further development of the Framework. For more info: https://www.nist.gov/cybersecurity-framework	United States	
ISA/IEC 62443	Originally called ANSI/ISA99, the International Society for Automation (ISA)/International Electrotechnical Commission (IEC) 62443 series provides guidance regarding improving and maintaining the cyber security of ICS. It includes technical reports, standards and recommended procedures, grouped by category. The first group, General, is for all entities responsible for manufacturing, implementing or managing ICS. The others are limited in their application, intended for owner/operators, integrators, and vendors, respectively. For more info: https://www.isa.org/	International	Industrial Automation

[2] https://www.congress.gov/bill/115th-congress/house-bill/2105

[3] https://www.congress.gov/bill/115th-congress/senate-bill/770

Conclusion

Constant vigilance

Security is a journey, not a destination. Organizations who embrace this are better equipped to achieve lasting improvement in their level of cyber security risk. Business and technology are dynamic and risk factors change frequently in response to both internal and external events. Cyber security programs need to continually look for new potential risks and periodically review past decisions to determine whether new information affects their assessments and actions taken. Collaboration in some capacity has to occur in order to truly cover all bases when it comes to cyber security; engaging OEMs and service providers is key. Organizations should therefore seek guidance among their peers, third parties, experts, and authorities in their cyber journey. With the growing awareness of cyber security challenges, and how to surmount these as outlined above, come opportunities for organizations to be successful in a dynamic digital age.

Contact us

Dee Kimata
Product Manager
Power Generation & Water

Jim Lemanowicz, GICSP
Director, Cyber Security
Power Generation & Water

abb.com/cybersecurity
abb.com/powergeneration
abb.com/water

Note:
We reserve the right to make technical changes to the products or modify the contents of this document without prior notice. With regard to purchase orders, the agreed particulars shall prevail. ABB does not assume any responsibility for any errors or incomplete information in this document.

We reserve all rights to this document and the items and images it contains. The reproduction, disclosure to third parties or the use of the content of this document – including parts thereof – are prohibited without ABB's prior written permission.