CONTROL

July 2014

ESSENTIALS OF CYBER SECURITY

Cyber security is an acknowledged and growing threat to the operational integrity of process manufacturing and other critical infrastructure sectors. Ensuring cyber security begins with assessment and remediation of the current state, but carries through to incident detection, management and continued assurance measures throughout an asset's lifecycle.

About the *Control Essentials* Series

The mission of the *Control Essentials* series is to provide process industry professionals with an up-to-date, top-level understanding of a range of key process automation topics. Our intent is to present essential engineering concepts in a practical, non-commercial fashion, together with a review of the latest technology and marketplace drivers—all in a form factor well suited for onscreen consumption. Check in at ControlGlobal.com/Essentials for other installments in the series.

—*The* Control *Editorial Team*

EXECUTIVE SUMMARY

The process industries have long been characterized by a conservative, belt-and-suspenders approach to safety. This is particularly true for technical professionals charged with the management of industrial control systems — including their connections to smart field devices, remote user applications, business systems and more.

Over the past several years, automation technology developers have leveraged commercial off-the-shelf technologies such as Microsoft Windows, Ethernet and Intel chips. These have helped to reduce development times and enhance enterprise interoperability and overall value for plant end users. Along the journey from proprietary to more open platforms, however, have come new complexities. Namely, the risks and realities of viruses, other malware and cyber terrorism.

The risks and complexities continue to grow. Companies must consider not only the cost and benefits but the cyber security of the automation components and systems they adopt.

How real is the threat? In October 2013, former U.S. Homeland Security Secretary Michael Chertoff told top oil and gas industry executives gathered at a summit in Houston, Texas, that it no longer takes an army to fight a war, as the top threat their businesses face in the future is not from physical risks, but cyber attacks. Since then, incidents have continued to proliferate. (Read more of what he had to say here.)

Fortunately, so have the solutions, including those specifically tailored to industrial process controls and systems. The first thing you can do is to get better acquainted with the latest trends, standards and technologies designed to keep you running safely — and sleeping soundly at night.

THE CYBER THREAT IN CONTEXT

A process automation system running without proper security measures faces an operational risk not unlike someone driving without automobile insurance. More to the point: Failing to address cyber security is as fraught with risk as ignoring key government standards and regulations, because a single incident of malware can compromise production quality and efficiency or worse, result in catastrophic losses in human and financial terms.

Security lapses can come from an office worker duped by a spoof or phishing email; a plant employee (disgruntled or otherwise) who introduces malware from an infected USB drive; a lax security guard who allows unauthorized access to an unauthorized person; or an engineer who makes an unauthorized modification to control logic and neglects proper log-in and documentation procedures. Even a seemingly innocuous USB drive can be the source of a major incident; this is thought to be the method by which the Stuxnet virus was introduced.

The cyber-arms race has escalated exponentially since the earliest computer viruses and antivirus software antidotes. Deliberate, malicious activities are now commonplace across the Internet, giving new relevance to the old saying, “Just because you’re paranoid, that doesn’t mean they aren’t out to get you.”

Threats come from many points of attack as new platforms emerge. Ostensibly harmless mobile “apps” have been found to contain malware; novice hackers with no programming knowledge have downloaded and used software “exploit kits” with preconfigured malware; sophisticated, organized crime and “hacktivist” groups can target particular companies or types of routers, servers, industrial controls and software. Any of these can target networks, systems and applications, from IT to industrial controls.

In the pre-Internet era, fears that bomb-making “how to” books could used by terrorists seem quaint by contemporary standards. Today, online tools such as the Shodan search engine expose site-specific industrial control system vulnerabilities to security professionals and attackers alike. In 2013, for instance, researchers in Finland used the search engine to find nearly 3,000 risk-exposed systems in the country’s water supply systems, building automation systems and more.

In the face of ongoing and increasingly sophisticated attacks, process and automation industry professionals, standards organizations and government bodies have organized their efforts. Their work is helping industrial plants face the cyber security issue with comprehensive standards, best practices and regulations.

INDUSTRY IN THE CROSSHAIRS

Control systems under threat include distributed control systems, programmable logic controllers and other systems that are often integrated with them such as safety-instrumented systems, plant performance management and asset management systems. Supervisory control and data acquisition systems, from factory controls to control-room applications to far-flung remote terminal units, have long been targets of cyber-hackers. Attackers have alternately gained physical access inside plants as well as remotely through Internet connections to target all manner of industrial systems:

In 2003, the "Slammer" SQL worm virus reportedly penetrated a network firewall at Ohio's Davis-Besse nuclear power plant and disabled a safety monitoring system for nearly five hours; the plant was operating without up-to-date security patches, among other issues.

In 2010, Stuxnet, a piece of Windows "zero day" malware, infected control systems to cause significant setbacks in Iran's nuclear program — and affected tens of thousands of systems across 155 countries. (More background from Network World and TechNewsWorld.)

In 2012, attackers released the Shamoon virus (a.k.a. Disttrack), disabling tens of thousands of Windows NT-based workstations at a major oil and gas producer. Fortunately, the effects were limited to a business network not connected to oil production, or the effects could have been catastrophic. Instances of "sibling" malware, including Duqu, continue to proliferate.

The 2014 Heartbleed exploit was based on a flaw in an OpenSSL library extension widely used in Web servers, embedded devices and industrial control systems. Other recent attacks have affected a broad range of industrial automation systems and applications. In some cases, researchers find vulnerabilities and agree to withhold making them public until a patch can be tested and deployed; in others, government advisories have been issued before patches are ready. In all cases, no vendor or user of computer technology is immune from a potential cyber security incident.

A LIFECYCLE COMMITMENT

Strategic corporate initiatives may have start dates, but once they start, the work is truly never done. Ongoing initiatives of include those for managing quality, safety, continuous improvement, sustainability and corporate responsibility.

And so it is with control system cyber security, which is maturing from a reactive mode to a more holistic management framework. This framework must address the entire project lifecycle of assessing and identifying risk, implementing strategies to protect or prevent against cyber intrusions, monitoring and detecting incidents, and responding and recovering from them. In addition, a properly managed program creates a feedback loop in which the control system (and facility) continually undergoes reassessment, just as any program designed for continuous improvement.

To better understand the lifecycle approach, consider some project key project phases. Early on, auditing and assessment identifies assets and uncovers vulnerabilities in the control system as well as allied systems and technologies (safety systems, asset management applications, closed circuit TV monitors, etc.). Vulnerabilities are then addressed via patches and antivirus measures, backup procedures, site/perimeter security improvements—whatever it takes. Speaking of whatever it takes, training and retraining are musts, and should start as early as possible.

The key to achieving a continuing, lifecycle approach to cyber security lies in the implementation of an overarching management plan. A sound management framework optimizes resources, identifies ongoing and emerging needs, improves compliance, coordinates personnel and makes remediation, prevention and response efforts more efficient and effective. This includes well-documented and comprehensive site-specific remediation processes, workflows and procedures for regular monitoring to ensure the plan is meeting its expected goals — and improving upon them. A comprehensive management plan provides a framework to measure, benchmark and continually improve prevention, protection, detection, mitigation, response and recovery. >>

The point in this condensed view of project steps is to emphasize that such practices are part of a new and enduring reality; the real work only begins when the implementation project ends. And because no control system security program can guarantee 100% protection against exploits yet unknown, the goal must therefore be to achieve what can be referred to as keeping risk "ALARP," or as low as reasonably practical. Cost-effectiveness is a valid consideration, from human resource allocations to technical and physical prevention and countermeasures to the cost of purchases and services from outside vendors. In addition to resource- and cost-effective activities in-house, organizations must also evaluate the effectiveness of the service and commitment of their external industrial control partners, such as systems integrators, consultants and control system vendors.

For example, a control system vendor should demonstrate its expertise and vigilance in supporting the project lifecycle. Disciplined leaders comply with accepted cyber security standards, test threat models, perform security analyses, conduct various tests of code (including use/abuse cases and under various data loads) and call upon independent sources to test the system for vulnerabilities before components are shipped. And for the lifecycle of an installation, they should have the capability to provide ongoing services such as training, on-site and remote support, periodic risk assessments and audits, security monitoring, rapid response to vulnerabilities and attacks.

In short, all stakeholders—in-house and external—share responsibility for cyber security.

ROADMAP RESOURCES

There is much work to do in an industrial control system cyber security program. As with other disciplines with broad scope, such as process safety management, established standards, best practices and regulations provide a roadmap to help organizations evolve from reactive to preventive, proactive strategies for risk management. Fortunately for process industry professionals, control system cyber security isn't the first issue requiring a disciplined approach to compliance with risk mitigation standards, including those that will eventually become international standards.

In many countries, standards become law, while in the U.S., agencies overseeing cyber security do so through arms-length, public-private partnerships. For instance, the U.S. Department of Homeland Security (DHS) partners with numerous public and private sector organizations to improve the nation's cyber infrastructure, and has spearheaded industry and control system-specific standards that carry practical the force of law. One source of such partnerships is The Critical Infrastructure Partnership Advisory Council (CIPAC), which engages groups such as the Chemical Sector Coordinating Council and other industry-led committees.

DHS' jurisdiction includes Chemical Facility Anti-Terrorism Standards (CFATS, or 6 CFR, Part 27) and more. DHS has authority to regulate the security of industrial facilities, which it has broken into 16 "Critical Infrastructure Sectors" that represent a high risk to national security. These sectors include chemical facilities — from petrochemical to pharmaceutical and consumer products — as well as nuclear, critical manufacturing (including primary metals), IT and communications and more. For some sectors, DHS cedes authority to other agencies, including: energy (DoE); water and wastewater (EPA); and food and agriculture (FDA and USDA). For each of these 16 groups, DHS has published a Sector-Specific Plan that goes beyond general IT concerns to cover industrial processes, with considerable attention to the industrial controls used in each industry. >>

While run by DHS, the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) is tightly partnered with private-industry process and control companies. It offers a wealth of resources, including recommended practices and supporting documents; and services beyond public reporting of security incidents. These include a lab to analyze malware and vulnerabilities in automation equipment; training; conferences; a downloadable "Cyber Security Evaluation Tool," based on work originally done by NIST; and an important clearinghouse function for the Industrial Control Systems Joint Working Group.

NERC, the North American Electric Reliability Corporation (NERC), whose mission is to ensure the reliability of the bulk power system in North America, was granted legal authority by the U.S. Congress to develop and enforce mandatory reliability standards for its constituent members, These include NERC CIP, a set of Critical Infrastructure Protection standards that range from training and sabotage reporting through recovery from incidents in is a not-for-profit international regulatory Authority. The National Institute of Standards and Technology (NIST) in February 2014 released is Version 1.0 of a voluntary Framework for Improving Critical Infrastructure Cybersecurity. This followed a year of consulting with DHS, Sector-Specific Agencies and others, including industry.

And the International Society for Automation (ISA) has developed a global standard ISA99, or IEC 62433, that is intended to unify terminology, codify control system security requirements and measures (similar to the safety-integrity levels developed for protective systems), and describe cyber security management best practices.

While each sector- and industry-specific standard will vary in its details, they all follow similar processes. They help plant owners and operators map existing processes, determine gaps and vulnerabilities, standard to prioritize resources, make improvements and maximize the impact of their cyber security and control system investments.

A JOURNEY, NOT A DESTINATION

Given the necessary lifecycle approach to cyber security, people are as critical to long-term success as are technologies and processes. But for many organizations, "people" issues are the hardest to manage.

Communication gaps can make or break a cyber security project. Beyond the traditional and perhaps still-lingering rivalries between engineering and IT departments in plant automation projects, security personnel must be considered equally as well as those from other functions in the organization. And unlike many other types of projects, the need to protect the privacy of employees plays a unique role in cyber security.

In fact, participants in the May 2014 NIST Privacy Engineering Workshop cited a "material communication gap" between policy, system/technology developers and engineers. All personnel in all disciplines must be made fully aware of the real risks at stake, lest a Big Brother mentality take hold and compromise long-term success. For its part, NIST is considering measures to establish a common terminology and an engineering framework with better-defined methods to aid in cross-functional team efforts.

The establishment of clear roles, responsibilities and areas of authority is key, and can be reinforced early on with comprehensive training. For example, detailed simulation exercises with real-world models of attack vectors and exploits can impart both technical and teamwork skills. Beyond training, there are many more opportunities to foster full engagement, including the following points offered by the DHS' Chemical Sector Coordinating Council:

- Ensure [that] one person takes ownership of ICS security and is accountable.
- Open the lines of communication between engineering, security, IT, process safety communities and manufacturing operations communities within your own company.
- Conduct an audit of current control system security measures and implement obvious fixes.
- Follow up with a control system security vulnerability analysis (risk assessment) for a complete identification of vulnerabilities and recommendations for corrective action.
- Implement a control system security management program that is integrated with existing company management systems for security, safety, quality, etc.

An additional factor is critical: senior management commitment. In many enterprises, top leadership fails to fully understand the need for, or extent of, cyber security and control system cyber security investments. Without it, IT, engineering and security leaders may have a difficult time truly applying and enforcing policies, especially if the program is seen as a threat to the status quo productivity of "normal" if less secure work processes.

Top management must be an integral piece of the communication loop in cyber security. The best programs and most secure operations are surely achieved by those for whom the commitment to cyber-security is universal across the facility and the entire organization.

MADE POSSIBLE BY

Honeywell

This Control Essentials guide on Cyber Security is made possible by Honeywell Process Solutions. The company's vendor-neutral cyber security services draw on its experience with more than 70 control system versions and hundreds of key industrial cyber security projects across the globe. It provides bottom-up, asset-based security risk management solutions customized to process control environments. The company's portfolio includes scalable tools, services, best practices, and support from Honeywell's global army of network- and security-certified personnel that secure users' critical infrastructure and deliver a more predictable and safe environment – regardless of control system vendor or location.

Learn more >>