How Test Labs Reduce Cyber Security Threats to Industrial Control Systems

by Pat Combs

Executive summary

Federal agencies are moving their industrial control systems (ICS) from operational business networks to separate, dedicated networks in order to enhance security. However, without a system to test the new equipment and software coming into these separate networks, security risks will persist. This paper explores the impact on security of instituting a sanctioned ICS test lab and recommends best practices for setting up and operating these labs.

998-2095-05-05-14AR0

Schneider Electric

Introduction

According to the Ponemon Institute's 2013 Cost of Cyber Crime Study, the average annualized cost of cyber crime was $11.6 Million in 2013 with an average time to resolve an attack of 65 days.[1] In the case of federal government agencies such as DOD, DOE, NNSA and DHS, the influence of cyber crime can also be measured in terms of lives when considering the critical nature of the infrastructure they support and manage. Industrial Control Systems (ICS) are essential to the operations of federal facilities and therefore play an important role in mitigating security risks to the networks.

The biggest threats to industrial control system (ICS) security are malware, inside actors, web attacks, SQL injection, and accidental failures. According to the ICS Cyber Emergency Response Team (ICS-CERT), a program of the Department of Homeland Security, 257 cyber incidents were reported in 2013 from across the 16 critical infrastructure sectors they support. This represents an increase of 30% vs. 2012[2].

Many federal agencies today recognize the threat and are beginning to secure their industrial control systems. Some are moving their control systems from the operational business networks into separate, dedicated ICS networks. Oftentimes these networks handle utility functions and business sensitive services. While such an approach represents a major step in the right direction, new security challenges based on operational business demands need to be addressed. A process for how vendors and employees receive approval to maintain and upgrade the control and management systems needs to be defined.

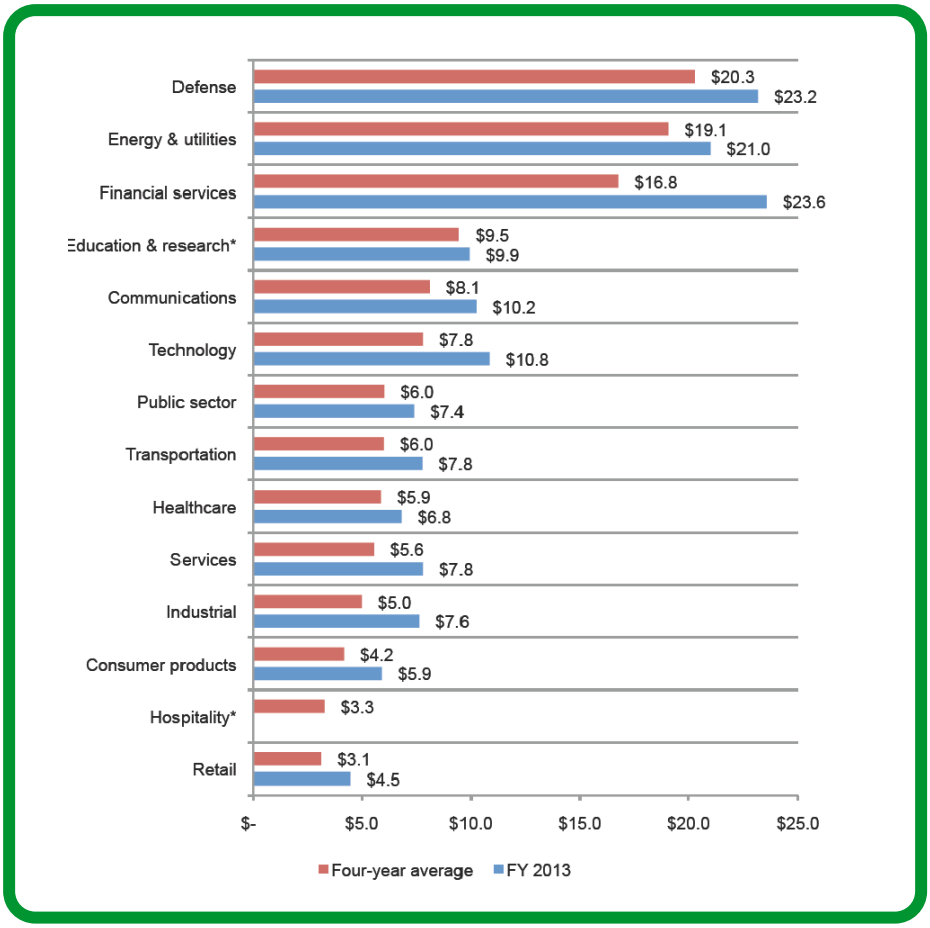

Figure 1
The average annualized cost of cyber crime varies by industry segment (courtesy of the Ponemon Institute)

[1] Ponemon Institute, "2013 Cost of Cyber Crime Study: United States", *Ponemon Institute Research Report*, page 2, 2013

[2] Industrial Control Systems Cyber Emergency Response Team, "ICS-CERT Year in Review 2013", Page 16, Table 2, 2014

This paper examines one important approach for maintaining a secure ICS operational environment: the deployment of DOD-accredited ICS labs for testing the equipment and software destined to reside in a dedicated ICS network. Such testing labs will assist network managers and operators in understanding how new hardware and software components behave in the network and to identify any inherent security threats. Test results can then allow management to make sound and secure business decisions and to approve or deny network access to the new hardware or software.

The purpose of an ICS lab is to test all elements of the business SCADA environment in order to:

1. Ensure that programmable logic controllers (PLCs), direct load controllers (DLCs), software, servers, and workstations are properly secured.
2. Prevent the ICS network from being used as an attack vehicle against the business network.

A typical ICS Lab requires approximately $150,000 of upfront capital investment. That cost needs to be weighed against the elevated risk of losing millions of dollars as the result of a cyber attack and also the potential threat to human lives.

Methodology

Test labs are built for multiple reasons. In pharmaceutical labs, tests expose how a drug reacts to a multitude of scenarios to better determine the side effects and potential benefits. In software labs, tests are conducted to identify errors and code behaviors when subjected to human interaction, multiple computer scenarios, or network architectures. An ICS Lab, tracks anomalies between quality assurance goals and vendor hardware / software products.

The ICS lab should be designed to identify the highest number of manufacturer defects in the shortest amount of time. Then, with each defect flagged, the type and level of risk for each defect should be identified. Note that fixing the defect is not within the scope or purpose of the ICS lab.

“By simulating the existing ICS topology, regression and stress testing can be performed to identify known and unknown faults or defects.”

Therefore the viability of each product that is considered as a potential candidate for integration into the ICS operational network is determined by how the following questions are answered:

- Does the product perform as intended?
- What does the product connect to?
- What type of testing is to occur? (Product, system, and / or enterprise?)
- What system interconnections occur between the product’s management system and others?
- Is this product critical to the ongoing function of the business?
- Do these systems rely on other control systems?

By answering these questions through the audit process, the ICS lab allows test engineers to reach factual conclusions based on firm data-driven results. Thus, any doubts as to whether the manufacturer’s product poses a risk or threat to the ICS operational network or whether it performs as stated are addressed.

Hardware and software audits

Industrial control system audits are performed on both hardware and on the software controlling the hardware (management software or firmware). Since industrial systems link many different components, it is critical to understand the application for which the technology is built. For example, some facilities use steam to heat buildings whereas others use steam to produce electricity. Other specialized facilities incorporate radiation detection

devices into their buildings while others use them as part of a campus-wide security system. Understanding the targeted application helps in better sanitizing the control systems equipment. The network topology is also an important consideration when designing the audit. Hardware and software audits should test using the same topology as found in the "live" ICS network, or as close as possible.

Software audits require a different set of hardware equipment to conduct the software tests. For example, test plans for the firmware residing inside of industry equipment are specifically for the firmware software and not the Energy Management System (EMS) software. Firmware software performs specific operations, receives specific analog and digital data points, and then passes it on to the EMS. The EMS system itself, on the other hand, is a server exposed to multiple threats because of its numerous hardware components and robust operation compared to a PLC's more simple hardware.

"Firmware is not built for security but for bolstering a vendor's product ease of use. This design approach results in vulnerabilities that leave applications open to cyber attacks."

Software audits require the use of a server equipped with the operating system currently being used in the "live" ICS network. Equipment must be as similar to existing operational equipment as possible. By simulating the existing ICS topology, regression and stress testing can be performed to identify known and unknown faults or defects which, in turn, can identify unknown hazards.

Management software is used to configure, implement, and maintain both the controllers and the sensors that reside downstream of the controllers. It is important to understand that not all EMS software operates the same way. HVAC system audits, for example, require the auditor to understand which controllers interact with the management software and which interact with the operating system (under which the management software resides).

Careful scrutiny and caution is needed during the preliminary analysis due to differences in how each EMS application functions. Firmware, for example, is not built for security but for bolstering a vendor's product ease of use. This design approach results in vulnerabilities that leave applications open to cyber attacks.

The audit should be conducted multiple times to understand how software processes are impacted, how other controllers in close proximity are affected, and whether network congestion occurs. For example, a vendor's meter firmware upgrade can be tested to identify potential data discrepancies or malfunctions prior to propagation across an ICS network of hundreds of identical meter models.

Reporting

A formal report should be produced once each item is fully tested. The process for the testing should be outlined and results from regression and stress tests should be posted. The report should include a series of recommendations and a final outcome statement that communicates whether or not the product is safe to deploy in the new dedicated network.

Conclusion

Over the past five years, ICS cyber attacks have escalated at a rate faster than many security analysts had expected. In fiscal year 2012, the ICS Cyber Emergency Response Team reported 193 known cyber incidents. By June of 2013 over 200 cyber incidents had been reported and the ICS Cyber Emergency Response Team had forecasted a doubling of incidents by the end of the year. The total for all of 2012 had already been surpassed by June of 2013. The amount of attacks increased 112% in just two years. Hackers are always gravitating towards the easiest systems to exploit and industrial control systems are now among the most popular hacking attack targets.

Stakeholders across manufacturing and governmental domains need to be aware of the security threats to their systems and of the solutions that are available in order to reduce those threats. If the internal Energy Management System (EMS) mechanisms are not tested and verified, there is no way of knowing how secure the EMS infrastructure really is. Systematic analysis of the system and its components will have to be performed. Otherwise, the system owners will be open to attacks on their industrial control system infrastructure.

About the author

Pat Combs is a 23-year veteran in the Industrial Control and cyber security industries. He has held numerous engineering and management positions throughout the US Federal Government and civilian industry and is currently the Schneider Electric U.S. Federal Government Solutions Architect. He has written multiple whitepapers, speaks at conferences on cyber security and Industrial Controls (IC) and is an active member of several industry associations, including SAME, EFCOG, US CERT ISJWG, SANS, ISC2, ISC West, and Energy Gov. He holds a BBA in Information Systems from James Madison University and a MS from University of Phoenix and is a certified CISSP, CGEIT, DAU Certified Level II in Program Management.