*The following 800 word article is available for media use:*

**The 7 Steps to ICS and SCADA Security**

The past two years have been a real wakeup call for the industrial automation industry. For the first time ever it has been the target of sophisticated cyberattacks like Stuxnet, Night Dragon and Duqu.

In addition, [an unprecedented number of security vulnerabilities](http://www.tofinosecurity.com/blog/s4-scada-security-symposium-takeaway-time-revolution) have been exposed in industrial control products and regulatory agencies are demanding compliance to complex and confusing regulations. Cyber security has quickly become a serious issue for professionals in the process and critical infrastructure industries.

If you are a process control engineer, an IT professional in a company with an automation division, or a business manager responsible for safety or security, you may be wondering how your organization can get moving on more robust cyber security practices.

In order to provide you with guidance in this area, we have condensed material from numerous industry standards and best practice documents. We also combined our experience in assessing the security of dozens of industrial control systems.

The result is an easy-to-follow 7-step process.

**The 7 Steps**

**Step 1 – Assess Existing Systems**

Your first step is to do a *risk assessment* to quantify and rank the risks that post a danger to your business. This is necessary so you know how to prioritize your security dollars and efforts. Far too often we see the assessment step skipped and companies throw money into a solution for a minor risk, leaving far more serious risks unaddressed.

While risk assessment might seem daunting, it can be manageable if you adopt a simple, lightweight methodology. Our white paper provides an example, as well as tips on how to do this.

**Step 2 – Document Policies and Procedures**

We highly recommend that organizations develop ICS-specific documents describing company policy, standards and procedures around control system security. These documents should refer back to corporate IT security documents. In our experience, separate ICS security documents greatly benefit those responsible for ICS security, helping them clearly understand their security-related expectations and responsibilities.

You should also become familiar with applicable security regulations and standards for your industry.

**Step 3 – Train Personnel & Contractors**

Once you have documented your policies and procedures, you need to make sure that your staff is aware of them and is following them. An awareness program should be carried out, with the support of senior management, to all applicable employees. Then, a training program should be conducted. We highly recommend a role-based training program for control systems security, and we provide an example of one in the white paper.

**Step 4 – Segment the Control System Network**

Network segmentation is the most important tactical step you can take to improve the security of your industrial automation system. Eric wrote about this in the article “[….No More Flat Networks Please…”](http://www.tofinosecurity.com/blog/controlling-stuxnet-%E2%80%93-no-more-flat-networks-please-lets-embrace-security-zones) The white paper explains the concepts of “zones” and “conduits” and provides a high level network diagram showing them.

**Step 5 - Control Access to the System**

Once you've partitioned your system into security zones, the next step is to control access to the assets within those zones. It is important to provide both physical and logical access controls.

Typical physical access controls are fences, locked doors, and locked equipment cabinets. The goal is to limit physical access to critical ICS assets to only those who require it to perform their job.

The same concepts apply to logical access control, including the concept of multiple levels of control and authentication. Once authenticated, users can be authorized to perform certain functions.

**Step 6 – Harden the Components**

Hardening the components of your system means locking down the functionality of the various components in your system to prevent unauthorized access or changes, remove unnecessary functions or features, and patch any known vulnerabilities.

This is especially important in modern control systems which utilize extensive commercial off-the-shelf technology. In such systems, it is critical to disable unused functions and to ensure that configurable options are set to their most secure settings.

**Step 7 – Monitor & Maintain System Security**

As an owner or operator of an industrial control system, you must remain vigilant by monitoring and maintaining security throughout the lifecycle of your system. This involves activities such as updating antivirus signatures and installing security patches on Windows servers. It also involves monitoring your system for suspicious activity.

Finally, it is important to periodically test and assess your system. Assessments involve periodic audits to verify the system is still configured for optimal security as well as updating security controls to the latest standards and best practices.

**Not a One-Time Project**

Now the bad news - effective ICS and SCADA security is not a one-time project. Rather it is an ongoing, iterative process. You will need to repeat the 7 steps and update materials and measures as systems, people, business objectives and threats change.

Your hard work will be rewarded with the knowledge that your operation has maximum protection against disruption, safety incidents and business losses from modern cyber security threats.

Download the White Paper “[7 Steps to ICS and SCADA Security](http://web.tofinosecurity.com/webtofinosecuritycom/download-7-steps)”

[(http://web.tofinosecurity.com/webtofinosecuritycom/download-7-steps)](http://web.tofinosecurity.com/webtofinosecuritycom/download-7-steps" \t "_blank)

**Authors**

|  |  |
| --- | --- |
| Eric Byres, P. Eng., ISA Fellow  CTO and VP Engineering  Tofino Security,  part of Hirschmann, a Belden Brand  eric.byres@tofinosecurity.com  www.tofinosecurity.com | John Cusimano, CISSP, CFSE  Director of Security  exida Consulting LLC  jcusimano@exida.com  www.exida.com |

**Related Link**

# Press Release: [Belden Responds to Sophisticated Cyber Threats on Critical Industrial Infrastructure](http://www.tofinosecurity.com/article/belden-responds-sophisticated-cyber-threats-critical-industrial-infrastructure)

Eric Byres, P. Eng., ISA Fellow, CTO and VP Engineering, Tofino Security, a subsidiary of Belden Inc., eric.byres@tofinosecurity.com, www.tofinosecurity.com