# The Supply Chain is Expanding the Attack Surface on your ICS

**Author: Daniel Ehrenreich, Consultant and Lecturer, SCCE**

## Overview

*Industry experts worldwide dealing with Industrial Control Systems (ICS) recognize the famous Stuxnet attack in 2010 (compromising a nuclear facility) as the formal starting point for dealing with cyber security. Until then, this concern did not get proper attention of vendors and neither users and only top class classified organizations implemented early-stage cyber defense solutions. The real game changer was triggered around 2014-2015, when several organizations worldwide suffered from real cyber-attacks.*

*Among these were externally generated attacks on the ICS through the IT zones of the organization and also internally cyber-attacks done by disgruntled employees, external service people and others, who had authorized access to the ICS. Industry experts worried about these risks, but until the famous Target chain attack in 2013, caused by negligent processes of their subcontractor, the attention was minimal.*

*This paper, specifically focusing on risks created by the supply chain, and outlines several considerations and scenarios which jointly combine to the term "attack surface". Obviously, the wider is the attack surface, the higher are the chances of cyber-attack against your organization.*

## Attention to ICS cyber risks

Experts can prepare a meaningful list of cyber risks however, the reality is that the management prefers talking about business continuity and profitability, rather than about risks. Therefore, the key topics presented to management shall refer to mitigating the ability of adversaries to interrupt the business continuity and presenting them detailed processes for fast and effective recovery from an incident.

Following are few examples pointing to risks caused by the technical supply chain. Understanding the consequences of these risks, may help you defining and deploying risk mitigation measures, which were specifically defined to restore business continuity in your organization.

1. Suppliers of Computer hardware and software
   - Purchase of computers, especially maintenance laptops shall be done from a reliable source. These shall be sealed in an original package and preferable without the operating systems installed.
   - All software licenses shall be obtained on an originally sealed CD, and installed at the facility of the organization after these computers were completely sanitized.
   - Special attention is required for purchasing maintenance software. Its periodic update process shall include receiving from the producer a sealed CD, and installed without internet connection.
2. PLC/ RTU hardware and Software
   - Large organizations' material departments often purchase through a tender process which allows adversaries to propose the requested product at a reduced cost.
   - To prevent such risk, the tender document shall specify that only original vendors or their authorized distributor may submit a proposal and deliver the product in an originally sealed package.
   - Furthermore, it is critical that the manufacturer's default user name and passwords (such as "admin-admin") will be changed. All previously used credentials shall be permanently deleted.
3. ICS Operation software programs
   - Among components often used in ICS networks, you may find managed switches, firewalls, unidirectional gateways, network monitoring and port mirroring devices, etc.
   - The software in the supplied products shall be completely deleted and the product shall be sanitized. All operation programs must be installed from a sealed original CD at the customers' facility.
   - Software updates shall never be done through the internet but always done locally. Prior any software is modified/updated the person in charge shall verify its operation on a test-bed.

4. Maintenance of ICS processes
   - ICS operations are definitely not a static process as things often require changes and adaptations, such as adding another sensor, another PLC or optimizing the process.
   - The question ICS managers will always ask: “who is capable doing it?”. In large organizations there is a team available and their role includes perioding maintenance and support.
   - But what small and medium size SMB) operation shall do? In most cases they rely on an external service provider who do it locally but very often they prefer doing it remotely.
5. Remote access for upgrades and repairs
   - Remote access to the ICS requires predefined connection via the public internet or a cellular modem. In such high-risk process, it is connected to the heart of the ICS, and can be seen as a “backdoor”.
   - Experts know well that these remote “sessions” represent a risk to the ICS, but they allow that because otherwise the plant manager cannot assure operation continuity.
   - Today, experts aware of risks caused by remotely connecting a service computer to their ICS. That PC might be infected during one of remote connections to the system of another client.

## Qualifying your supply chain

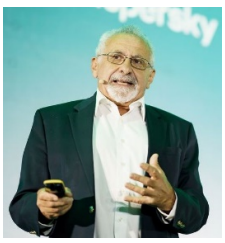
The “supply chain cyber risk” term refers to a broad range of vendors, partners, service providers, etc. Among these can be large and well managed organizations but also smaller vendors who work correctly and use security certificates which allow them securely maintaining your network. Obviously the easiest could by working only with suppliers which consistently comply with the ISO 27001-2013, but, as long as this is not a country-wide mandatory regulation, it will be difficult to enforce that process. Until things change and regulations become mandatory, you may start qualifying your vendors with a short and manageable list of questions. While this is not a complete process it is a good start towards future improvements:

- Is your vendor listed as a supplier to top class companies, or are they among such companies?
- How effectively will they react when a zero-day vulnerability is published affecting your system?
- Do they have a training program for their employees including CISSP or similar certification?
- Which other local and international customers use their service? How did they qualify them?
- Are they willing to allocate dedicated tools for supporting your system or use your PC tools?
- How they qualify their employee’s prior hiring them? How often they revisit that process?
- For quality assurance, is their support process; Documented, Repeatable, Measurable?
- How they protect your software? Are physical security measures deployed in their facility?

## Summary

Enhanced cyber defense is achievable through adherence to the PPT Triad (People, Policies and Technology). Of course, the best situation could be that organizations have their own employees, but in most SMB, it is not realistic. Therefore, they shall consider the PPT process which is applicable and manageable for the list of suppliers which they must employ. The meaning of that process is that all acting people must be trained to the required expertise, technology solutions must be carefully tuned for the level of risk and impact, organization policies must be defined and enforced. While no single solution may absolutely protect your organization, adherence to these principles will put you a step ahead of the attackers.

@@@@@@



**Daniel Ehrenreich, BSc.** is a consultant and lecturer acting at Secure Communications and Control Experts, and periodically teaches in colleges and present at industry conferences on integration of cyber defense with industrial control systems; Daniel has over 27 years’ engineering experience with ICS and OT/IIoT systems for: electricity, water, gas and power plants as part of his activities at Tadiran, Motorola, Siemens and Waterfall Security. Acting as the permanent Chairman for the ICS Cybersec annual conference in Israel. *LinkedIn*