Homeland Security

NCCIC

National Cybersecurity and Communications Integration Center

## INTRODUCTION

Cyber intrusions into US Critical Infrastructure systems are happening with increased frequency. For many industrial control systems (ICSs), it's not a matter of *if* an intrusion will take place, but *when*. In Fiscal Year (FY) 2015, 295 incidents were reported to ICS-CERT, and many more went unreported or undetected. The capabilities of our adversaries have been demonstrated and cyber incidents are increasing in frequency and complexity. Simply building a network with a hardened perimeter is no longer adequate. Securing ICSs against the modern threat requires well-planned and well-implemented strategies that will provide network defense teams a chance to quickly and effectively detect, counter, and expel an adversary. This paper presents seven strategies that can be implemented today to counter common exploitable weaknesses in "as-built" control systems.

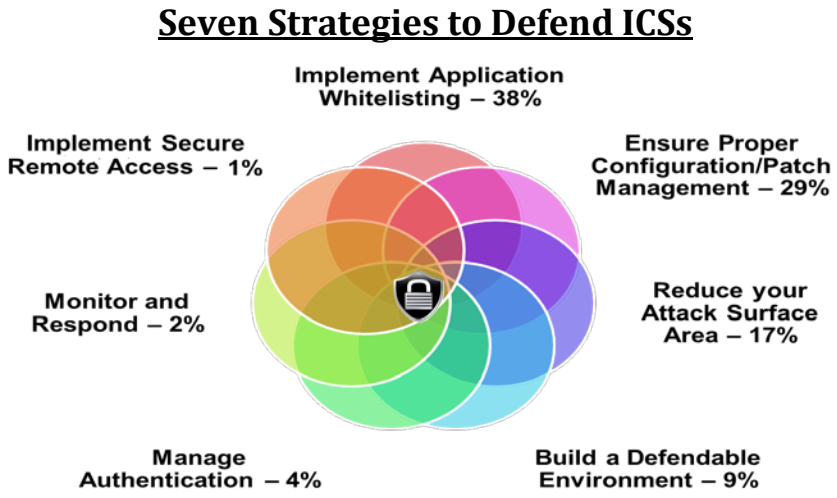


Figure 1: Percentage of ICS-CERT FY 2014 and FY 2015 Incidents Potentially Mitigated by Each Strategy[a]

a. Incidents mitigated by more than one strategy are listed under the strategy ICS-CERT judged as more effective.

If system owners had implemented the strategies outlined in this paper, 98 percent of incidents ICS-CERT responded to in FY 2014 and FY 2015 would have been prevented. The remaining 2 percent could have been identified with increased monitoring and a robust incident response.

## THE SEVEN STRATEGIES

### 1. IMPLEMENT APPLICATION WHITELISTING

*Application Whitelisting (*AWL) can detect and prevent attempted execution of malware uploaded by adversaries. The static nature of some systems, such as database servers and human-machine interface (HMI) computers, make these ideal candidates to run AWL. Operators are encouraged to work with their vendors to baseline and calibrate AWL deployments.

> **Example:** ICS-CERT recently responded to an incident where the victim had to rebuild the network from scratch at great expense. A particular malware compromised over 80 percent of its assets. Antivirus software was ineffective; the malware had a 0 percent detection rate on VirusTotal. AWL would have provided notification and blocked the malware execution.

### 2. ENSURE PROPER CONFIGURATION/PATCH MANAGEMENT

Adversaries target unpatched systems. A configuration/patch management program centered on the safe importation and implementation of trusted patches will help keep control systems more secure.

Such a program will start with an accurate baseline and asset inventory to track what patches are needed. It will prioritize patching and configuration management of "PC-architecture" machines used in HMI, database server, and engineering workstation roles, as current adversaries have significant cyber capabilities against these. Infected laptops are a significant malware vector. Such a program will limit connection of external laptops to the control network and preferably supply vendors with known-good company laptops. The program will also encourage initial installation of any updates onto a test system that includes malware detection features before the updates are installed on operational systems.

> **Example:** ICS-CERT responded to a Stuxnet infection at a power generation facility. The root cause of the infection was a vendor laptop.

Use best practices when downloading software and patches destined for your control network. Take measures to avoid "watering hole" attacks. Use a web Domain Name System (DNS) reputation system. Get updates from authenticated vendor sites. Validate the authenticity of

downloads. Insist that vendors digitally sign updates, and/or publish hashes via an out-of-bound communications path, and use these to authenticate. Don't load updates from unverified sources.

> **Example:** HAVEX spread by infecting patches. With an out-of-band communication path for patch hashes, such as a blast email, users could have validated that the patches were not authentic.

## 3. REDUCE YOUR ATTACK SURFACE AREA

Isolate ICS networks from any untrusted networks, especially the Internet.[b] Lock down all unused ports. Turn off all unused services. Only allow real-time connectivity to external networks if there is a defined business requirement or control function. If one-way communication can accomplish a task, use optical separation ("data diode"). If bidirectional communication is necessary, then use a single open port over a restricted network path.

> **Example:** As of 2014, ICS-CERT was aware of 82,000 cases of industrial control systems hardware or software directly accessible from the public Internet. ICS-CERT has encountered numerous cases where direct or nearly direct Internet access enabled a breach. Examples include a US Crime Lab, a Dam, The Sochi Olympic stadium, and numerous water utilities.

## 4. BUILD A DEFENDABLE ENVIRONMENT

Limit damage from network perimeter breaches. Segment networks into logical enclaves and restrict host-to-host communications paths. This can stop adversaries from expanding their access, while letting the normal system communications continue to operate. Enclaving limits possible damage, as compromised systems cannot be used to reach and contaminate systems in other enclaves. Containment provided by enclaving also makes incident cleanup significantly less costly.[c]

b. ICS-ALERT-14-063-01AP, Multiple Reports of Internet Facing Control Systems, ICS-CERT 2015.

c. Improving Industrial Control Systems Cybersecurity with Defense in Depth, ICS-CERT 2009.

**Example:** In one ICS-CERT case, a nuclear asset owner failed to scan media entering a Level 3 facility. On exit, the media was scanned, and a virus was detected. Because the asset owner had implemented logical enclaving, only six systems were put at risk and had to be remediated. Had enclaving not been implemented, hundreds of hosts would have needed to be remediated.

If one-way data transfer from a secure zone to a less secure zone is required, consider using approved removable media instead of a network connection. If real-time data transfer is required, consider using optical separation technologies. This allows replication of data without putting the control system at risk.

**Example:** In one ICS-CERT case, a pipeline operator had directly connected the corporate network to the control network, because the billing unit had asserted it needed metering data. After being informed of a breach by ICS-CERT, the asset owner removed the connection. It took the billing department 4 days to notice the connection had been lost, clearly demonstrating that real-time data were not needed.

## 5. MANAGE AUTHENTICATION

Adversaries are increasingly focusing on gaining control of legitimate credentials, especially those associated with highly privileged accounts. Compromising these credentials allows adversaries to masquerade as legitimate users, leaving less evidence than exploiting vulnerabilities or executing malware. Implement multi-factor authentication where possible. Reduce privileges to only those needed for a user's duties. If passwords are necessary, implement secure password policies stressing length over complexity. For all accounts, including system and non-interactive accounts, ensure credentials are unique, and change all passwords at least every 90 days.

Require separate credentials for corporate and control network zones and store these in separate trust stores. Never share Active Directory, RSA ACE servers, or other trust stores between corporate and control networks.

**Example:** One US Government agency used the same password across the environment for local administrator accounts. This allowed an adversary to easily move laterally across all systems.

## 6. IMPLEMENT SECURE REMOTE ACCESS

Some adversaries are effective at gaining remote access into control systems, finding obscure access vectors, even "hidden back doors" intentionally created by system operators. Remove such accesses wherever possible, especially modems as these are fundamentally insecure.

Limit any accesses that remain. Where possible, implement "monitoring only" access enforced by data diodes, and do not rely on "read only" access enforced by software configurations or permissions. Do not allow remote persistent vendor connections into the control network. Require any remote access be operator controlled, time limited, and procedurally similar to "lock out, tag out." Use the same remote access paths for vendor and employee connections; don't allow double standards. Use two-factor authentication if possible, avoiding schemes where both tokens are similar types and can be easily stolen (e.g., password and soft certificate).

**Example:** Following these guidelines would have prevented the BlackEnergy intrusions. BlackEnergy required communications paths for initial compromise, installation and "plug in" installation.

## 7. MONITOR AND RESPOND

Defending a network against modern threats requires actively monitoring for adversarial penetration and quickly executing a prepared response.

Consider establishing monitoring programs in the following five key places:

1) Watch IP traffic on ICS boundaries for abnormal or suspicious communications.
2) Monitor IP traffic within the control network for malicious connections or content.
3) Use host-based products to detect malicious software and attack attempts.
4) Use login analysis (time and place for example) to detect stolen credential usage or improper access, verifying all anomalies with quick phone calls.
5) Watch account/user administration actions to detect access control manipulation.

Have a response plan for when adversarial activity is detected. Such a plan may include disconnecting all Internet connections, running a properly scoped search for malware, disabling affected user accounts, isolating suspect systems, and an immediate 100 percent password reset. Such a plan may also define escalation triggers and actions, including incident response, investigation, and public affairs activities.

Have a restoration plan, including having "gold disks" ready to restore systems to known good states.

**Example:** Attackers render Windows®[d] based devices in a control network inoperative by wiping hard drive contents. Recent attacks against Saudi Aramco™[e] and Sony Pictures demonstrate that quick restoration of such computers is key to restoring an attacked network to an operational state.

## CONCLUSION

Defense against the modern threat requires applying measures to protect not only the perimeter but also the interior. While no system is 100 percent secure, implementing the seven key strategies discussed in this paper can greatly improve the security posture of ICSs.

## DISCLAIMER

The information and opinions contained in this document are provided "as is" and without any warranties or guarantees. Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by the United States Government, and this guidance shall not be used for advertising or product endorsement purposes.

## ACKNOWLEDGMENT

This document "Seven Steps to Effectively Defend Industrial Control Systems" was written in collaboration, with contributions from subject matter experts working at the Department of Homeland Security (DHS), the Federal Bureau of Investigation (FBI), and the National Security Agency (NSA).

d. Windows® is a registered trademark of Microsoft Corp.

e. Saudi Aramco™ is an unregistered trademark of Saudi Arabian Oil Company.

## CONTACT INFORMATION

| POC | Phone | e-Mail |
|---|---|---|
| Department of Homeland Security<br>ICS-CERT | 877-776-7585 | ICS-CERT@HQ.DHS.GOV |
| Federal Bureau of Investigation<br>Cyber Division - CyWatch | 855-292-3937 | tciu@ic.fbi.gov |
| National Security Agency (Industry)<br>Industry Inquiries | 410-854-6091 | bao@nsa.gov |
| National Security Agency (Government)<br>IAD Client Contact Center | 410-854-4200 | IAD_CCC@nsa.gov |