7 U.S. Homeland Security Strategies + 7 Ways GE Power Digital Solutions Respond

290
of 296 incidents mitigated

Of the **296 incidents** that the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) responded to in 2015, **98% could have been mitigated by following seven security control practices.** The other 2% could have been identified using basic monitoring.

Cyber intrusions into utility infrastructures are on the rise globally. Reliance on an ever-growing network of software, devices and interconnected remote systems brings new risks to the global power supply daily. Energy and government experts agree that if utilities continue to embrace digital infrastructure without implementing important security measures, a major compromise will be imminent.

The United States Department of Homeland Security, through the release of its **Seven Strategies to Defend Industrial Control Systems (ICSs)**, has sounded the alarm. Power producers around the globe are urged to respond quickly to implement the needed security recommendations. Waiting is no longer considered an option – producers must proactively strengthen their defenses, monitoring and response mechanisms today.

This information sheet can help global power operators and IT professionals understand the implications of the seven recommendations and how GE Power Digital Solutions can help to achieve them.

GE Power Digital

HOMELAND SECURITY STRATEGY #1:

Implement Application Whitelisting

A commonly used tactic for infiltrating an organization's systems has been through email phishing campaigns that install malware on an employee's computer. This malware can open a back door, an important first step on the path to gain access to control systems.

Application whitelisting should be the first line of defense for any utility wanting to prevent malware from getting an opportunity to run or install. When properly configured, it proactively stops most malware, even those of an unknown nature. Through whitelisting any program that doesn't have permission or behaves in a way not expected simply does not have a chance to penetrate into the operating environment.

GE Power Digital Solutions:

OpShield: Provides the ability to do network and application level whitelisting and blacklisting.

SecurityST: An additional option for application level whitelisting and blacklisting.

HOMELAND SECURITY STRATEGY #2:

Ensure Proper Configuration/Patch Management

An additional step to help prevent the execution and spread of viruses and malware is to make sure all potential points of entry within a utility stay current on antivirus capabilities.

Attackers are skilled at evolving their methods of malware and viruses. And if a utility is lax about updating any point of entry, including HMIs and devices, these can easily become weaknesses. Maintaining proper configuration and patch management can catch viruses and malware before widespread damage is done.

GE Power Digital Solutions:

Cyber Asset Protection (CAP) Program: Determines if HMIs and other network devices are patched with validated and tested patches and have up-to-date antivirus signatures.

SecurityST: Automates the patching and antivirus signature management process and provides the ability to implement 260 hardening settings.

HOMELAND SECURITY STRATEGY #3:

Reduce Your Attack Surface Area

Any piece of systems infrastructure adds to a utility organization's risk. Unneeded services provide extra surface attack area — and can provide communication entry points for attackers. Because of this, utilities need to make sure that any component that is a part of their control system or that attaches to their control system is actually required. Additionally, what is connected should only be allowed to communicate in a very controlled way.

One way-communications can protect a system by assuring that that inbound communication is gated and controlled to prevent messaging that might be risky, while still allowing for unimpaired listening. A central egress methodology for connecting to untrusted networks is also important, this will lessen the likelihood that unwanted communication gets through a utility's line of defense through a weak or unmonitored entry point.

Hardening of systems provides additional security. Ironically, there may be a temptation to add additional services to harden, segment and control when in the end these additional services may translate to additional risk. Because of this paradox, it is important to build security thoughtfully and holistically.

GE Power Digital Solutions:

OpShield: Enforces communication policies and can be used to build one-way communications protection.

NetworkST: Uses a central egress methodology for connecting to untrusted networks.

Professional Services: Provides the expertise to support a planned and holistic hardening approach — one that can successfully protect against attacks without adding unnecessary surface area.

HOMELAND SECURITY STRATEGY #4:

Build a Defendable Environment

Without segmented and gated access, once an attacker has entered a utility system they can easily move through different areas until they are able to gain access to the control center. This access can be gained through any system or device that is connected and communicating to your network.

Building a defendable environment means creating gates that don't allow one point of entry to lead to other areas of a system if not needed. This approach should be considered across the spectrum of a utility's system, not just for a single network but also for every component in the control system and everything that connects to the control system. A comprehensive segmentation of all touch points with enforced data flows and established check points can build the protection into an environment that will keep important areas secure even if a breach occurs within a related area.

GE Power Digital Solution:

OpShield: Supports logical network segmentation that creates zones as well as enforces communication data flows into, out of and throughout the network. OpShield also enables whitelist policy association to specific zones.

HOMELAND SECURITY STRATEGY #5:

Manage Authentication

Once an attacker infiltrates a system they can easily work to compromise user names and passwords, escalating privileges as they move through a utility's networks until they finally have control over system networks used to manage and monitor grid operations.

There are several ways to manage authentication to avoid this type of access. User authentication and role-based access policies ensure that only individuals that truly need to have access to segmented areas are able to gain it. And when they do have access, strong two-step authentication and password controls makes sure that they really are who they say they are. Additionally, a centralized user account administration can eliminate the risks involved with account credential setup and maintenance on each individual host — a practice that can create extra room for error and in-turn opportunity for hackers.

GE Power Digital Solutions:

SecurityST: Features an Active Directory component that enables utilities to build user authentication and administer user accounts centrally.

Professional Services: Partners with utilities to develop the role-based access policies.

HOMELAND SECURITY STRATEGY #6:

Implement Secure Remote Access

Weakly secured remote access is like leaving the front door of a utility system wide open. Attackers can easily gain access and establish control. An attacker with control of grid operator workstations can open circuit breakers and take them offline — all from the comfort of their own remote location anywhere in the world.

Obviously, organizations should limit remote access to control system networks. If remote access is needed it should be time-limited and controlled using two-factor authentication and access control policies.

Utilities should identify existing and potential remote access points, block and disconnect from unneeded access points and implement security around all required points. Access should be diligently monitored to determine who is connecting and what they are doing. The least amount of permissions necessary should be granted with fundamental laws over permissions.

GE Power Digital Solutions:

PDS Health Check: Provides support for utilities needing to identify existing and potential remote access points.

OpShield: Secures remote access points.

SecurityST: Provides two-factor authentication and access control policies that are further needed to keep remote access point secure.

HOMELAND SECURITY STRATEGY #7:

Monitor and Respond

Naturally an attacker will have a much easier time of it if a utility is not paying attention to its networks, monitoring who is entering and what they are doing. Keeping a close eye on activity near and within a control system makes complete sense.

Monitoring systems that alert on attacks and anomalies on all protected equipment really are a necessity. Host-based intrusion detection and remote monitoring and diagnosis are also important. And while holistic monitoring and analysis that leverages all available data is an important first step, prepared response is needed to work in conjunction. Utilities need to establish procedures ahead of time so that when something does go wrong they can deploy a solution at a moment's notice.

GE Power Digital Solutions:

OpShield: Provides alerts on both attacks and anomalies initiated using supporting device communication protocols.

Cyber Asset Protection (CAP) Program: Includes host-based intrusion detection.

MSSP: Allows remote monitoring and diagnostics of GE customer systems.

SecurityST and Saber: Act as a Security Information Event Monitor (SIEM) to collect information and data and analyze it for potentially high-risk behaviors.

Conclusion

The complexity of staying secure is growing as utilities add more digital functionality and expand into dispersed networks. The risk of a cyber attack that could impact a global power grid is very much real — as demonstrated by the United States Department of Homeland Security's Seven Strategies recommendations.

GE Power Digital is ready to partner with you as you begin to navigate how to build these security recommendations in your utility operations.

Learn more about our solutions. Go to: www.gepower.com or call 1-855-your1GE.

QUICK GUIDE

GE Power Digital Solutions Directly Solve for Each Homeland Security Strategy

Homeland Security Strategy	GE Power Digital Solutions
Implement Application Whitelisting	**OpShield.** Provides the ability to do network- and application-level whitelisting and blacklisting. **SecurityST.** Additional option for application-level whitelisting and blacklisting.
Ensure Proper Configuration/ Patch Management	**Cyber Asset Protection (CAP) Program.** Determines if HMIs and other network devices are patched and have up-to-date antivirus signatures. **SecurityST.** Automates the patching and antivirus signature management process and provides the ability to implement 260 hardening settings.
Reduce Your Attack Surface Area	**OpShield.** Enforces communication policies and can be used to build one-way communications protection. **NetworkST.** Uses a central egress methodology for connecting to untrusted networks. **Professional Services**. Provides the expertise to support a planned and holistic hardening approach — one that can successfully protect against attacks without adding unnecessary surface area.
Build a Defendable Environment	**OpShield.** Supports logical network segmentation that creates zones as well as enforces communication data flows into, out of and throughout the network. OpShield also enables whitelist policy association to specific zones.
Manage Authentication	**SecurityST.** Features an Active Directory component that enables utilities to build user authentication and administer user accounts centrally. **Professional Service.** Partners with utilities to develop the role-based access policies.
Implement Secure Remote Access	**PDS Health Check.** Provides support for utilities needing to identify existing and potential remote access points. **OpShield.** Secures remote access points. **SecurityST.** Provides additional two-factor authentication and access control policies needed to keep remote access points secure.
Monitor and Respond	**OpShield.** Provides alerts on both attacks and anomalies initiated using supporting device communication protocols. **Cyber Asset Protection (CAP) Program.** Includes host-based intrusion detection. **MSSP.** Allows remote monitoring and diagnostics of GE customer systems. **SecurityST and Saber.** Act as a Security Information Event Monitor (SIEM) to collect information and data and analyze it for potentially high-risk behaviors.

For information on GE Power Digital Solutions:
www.ge.com/digital/power

Tel: **1-855-your1GE**
Email: **gedigital@ge.com**