Mitigating Cyber Risk Exposure

Digital Solutions for Cyber Security

GE Digital

Cyber Security — The Time to Act is Now

Traditional risk management is focused on factors like fluctuation in renewables dispatch priority and dynamic fuel costs. Today, the threat of cyber-attack and security breaches are equally prominent issues that can quickly cascade into serious financial damage or impact on human safety.

In 2014, the Pew Research Center predicted that a major industrial cyber-attack will occur in the US sometime within the next 10 years.* With the world demanding 50% more electricity in that same time frame,** power infrastructure will grow, and with it, the threat of cyber-attacks.

Cyber security has become a corporate board-level priority and a required investment for power leaders globally.

"To the extent that cyber events can disrupt safety or availability, ICS cyber security is quickly emerging as a top priority."

— Bengt Gregory-Brown and Derek Harp November, "A SANS Whitepaper", The Sans Institute, 2016

64% of power and utilities believe that their security strategy is not aligned with today's risk environment. *Source: Ernst & Young.*

SECURITY THREATS HAVE BECOME A FACT OF LIFE FOR UTILITIES

400%
increase in disclosed ICS attacks between 2010 and 2012

229 days
average length of time that breaches go unidentified

84%
of cyber attacks target software applications

*Source: Pew Research Center
**Source: GE Power

The Impacts Are Great

In the Ukraine, **225K** people lost power due to cyber attack in December 2015 — and again in December 2016.

$38B in damages from MyDoom virus, due to lost productivity, network downtime and compromised data.

Source: Investopedia, 2012 and PBS Frontline, 2000.

Unplanned disruptions cost **3%–8%** of capacity; **$10B** annual lost production.

Source: GE P&W

NERC CIP carries **$1M** per day fine for security compliance violation.

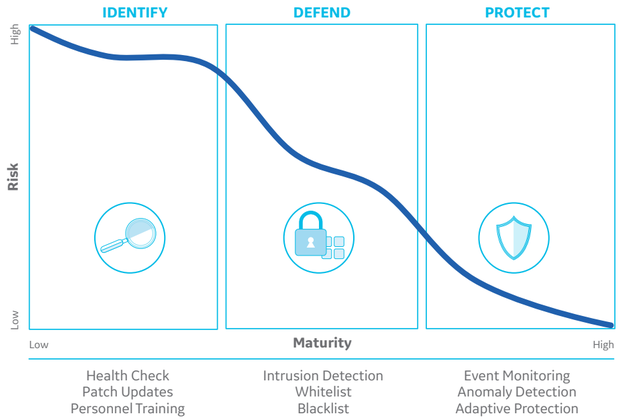
The Right Approach to Reduce Cyber Risk

Leaders who plan proactively along a maturity progression of “Identify, Defend, Protect” to address security vulnerabilities across their entire enterprise stand a better chance of reducing overall portfolio risk.

IDENTIFY
Immediate identification of anomalies indicating a cyber-attack, across connected and air gapped systems.

DEFEND
Implement security monitoring and defensive layers to comply with standards and strengthen the security posture.

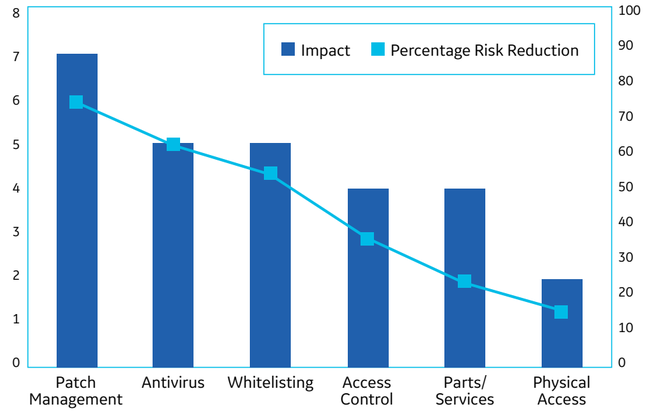
PROTECT
Pursue proactive and predictive security measures such as running attack scenarios on cloud-collected data. “Digital twins” can replicate operating environments and simulate defenses to measure threat impact and improve security.



UNDERSTAND WHICH STEPS TO TAKE FIRST

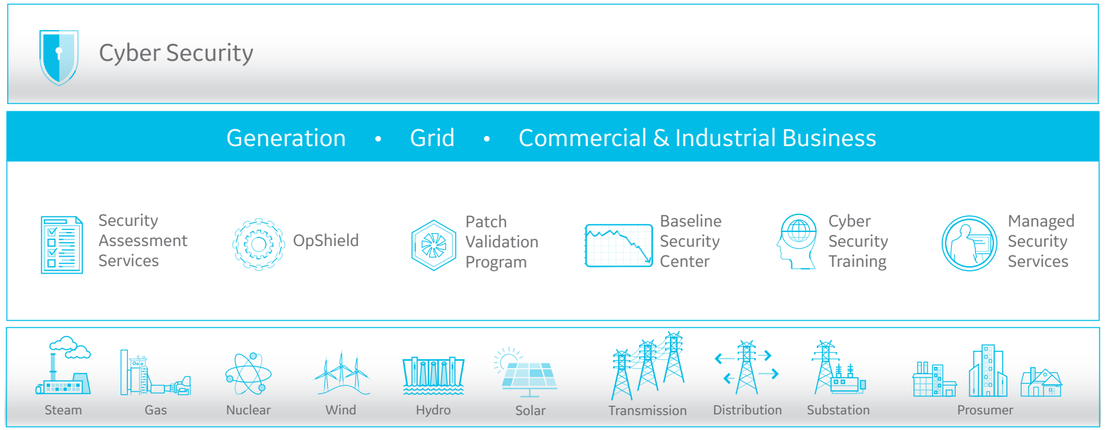
Understanding immediate threats and Implementing defensive measures to most effectively address vulnerabilities can help avoid compliance penalties and meet security standards deadlines, from NERC-CIP to IEC 62443-2-4 and ISO27000.

CENTER FOR INTERNET SECURITY THREAT/RISK ASSESSMENT



Source: Center for Internet Security

GE Power Digital Cyber Security Solution Suite



RESULTS OF GE ASSESSMENTS PERFORMED FOR POWER GENERATION

96% at least one system with a vulnerable OS

92% at least one system with an expired end-point solution

88% user access practices that do not align to industry best practices

96% at least one "dual-homed" systems (circumventing firewall)

8% at least one system where malware has been detected

0% effective Cyber Security monitoring

12+ years longest duration since administrator password

"Cyber incidents are inevitable in today's world. It's our job to understand what is most important to the business and manage the risk. If an incident does happen, proper response is key in determining the level of impact it will have on your business."

— Teresa Zielinski, CISO, GE Power

GE Cyber Security Solution Descriptions

Security Assessment Services

A portfolio of professional services to assess cyber security risk and prioritize remediation action, as well specialized NERC CIP and IEC 62443-2-4 compliance services.

GE security professionals perform hundreds of cyber vulnerability assessments globally. Specialists are highly qualified to perform both on-site and remote assessments.

OpShield

A purpose-built IDS/IPS security solution designed to protect critical infrastructure, control systems and operational technology (OT) assets.

OpShield monitors and alerts for malicious activity and minimizes disruptions to enable highly available operations and secure productivity.

Patch Validation Program (PVP)

Functional validation platform to reduce likelihood of patch deployments compromising availability.

Patch validation program leveraging application container technology to automate validation and deployment for OT controls HMI hosts

Baseline Security Center

A set of tools, configurations, and services focused on reduction of cyber risk and follows the Center for Internet Security's 20 Critical Security Controls.

Risk management platform that provides security tools, configurations, and practices to reduce exposure to cyber risk. Unlike typical vendor products, Baseline Security Center is platform agnostic.

Cyber Security Training

A comprehensive portfolio of security training courses for critical infrastructure and Industrial Control Systems (ICS) to increase staff knowledge and awareness.

Training content is developed and delivered by GE's security experts, who regularly analyze and implement real-world security solutions at operating facilities.

Managed Security Services

Strategic implementation of log aggregation capability to populate on premise SIEM and remote security operations capabilities.

Remote monitoring and diagnostics of OT control environment security events. Activities are examined on network, ICS, and host environments; user and systems accounts are monitored for malicious or compromising events.

CYBER ADOPTION ACROSS THE PLANT

Centrais Elétricas de Sergipe S.A. (CELSE), an independent power producer in Brazil, is adopting OpShield cyber security solution, a specialized internet-connected sharing firewall that helps protect critical infrastructure by monitoring and blocking malicious activity directed at plant assets.

"We are pleased this project incorporates the latest digital technology and security solution into our multiyear agreement with GE to help us ensure that our Porto de Sergipe plant operates at the highest levels of reliability and availability to support our power purchase agreements."

— Eduardo Maranhão, CEO of CELSE

7 US Homeland Security Imperatives: GE Solutions Span All Requirements

The United States Department of Homeland Security, through the release of its Seven Strategies to Defend Industrial Control Systems (ICSs), have indicated clear guidelines of the steps required to protect national access to uninterrupted power.

		OpShield	Baseline Security Center	Patch Validation Program	NetworkST	Professional Services	PDS Health Check	Managed Security Services
Implement Application Whitelisting	Application whitelisting is the first line of defense for any utility wanting to prevent malware breaches.	✓	✓					
Ensure Proper Configuration/ Patch Management	Ensure all potential points of entry within the environment stay current on antivirus capabilities.		✓	✓				
Reduce Attack Surface Area	Any component that is a part of a control system is actually required and what is connected should only be allowed to communicate in a very controlled way.	✓			✓	✓		
Build Defendable Environment	Create gates within the environment that don't allow one point of entry to lead to other areas of a system if not needed.	✓						
Manage Authentication	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.		✓			✓		
Implement Secure Remote Access	Utilities should identify existing and potential remote access points, block and disconnect from unneeded access points and implement security around all required points.		✓				✓	
Monitor and Respond	Monitoring systems that alert on attacks and anomalies on all protected equipment are a necessity.		✓	✓				✓

290 of **296**
incidents mitigated

Of the 296 incidents that the Industrial Control Systems 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.

GE Commitment to Cyber Security

EXECUTIVE MANAGEMENT

Jim Fowler
VP, GE CIO

Teresa Zielinski
CISO, GE Power

Robert Garry
Executive Chief Engineer, Cyber Security, GE Power

Tom Mueller
VP, Product Management, Predix Edge, GE Digital

Over **200** cyber assessment projects globally

250+ customers globally

10+ years
offering cyber security solutions and services

GE Digital | 1-855-your1GE | www.ge.com/digital/power-utility