Cyber Security Solutions

Mitigating cyber risk to drive power business growth

The complex demands of today's power business are driving leaders to invest substantial resources into business planning, with directed attention to risk mitigation. Over 90% of power executives believe top line growth can only be achieved through enhanced management of risk with the strategic adoption of technology.

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. They can cause trips, break operating limits, and 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[1]. With the world demanding 50% more electricity in that same time frame,[2] power infrastructure will grow, and with it, the threat of cyber attacks. Cyber security is a corporate board-level priority and a required investment for power leaders globally.

64% **of power and utilities believe that their security strategy is not aligned with today's risk environment.[3]**

A cohesive risk management approach

Leaders who plan proactively have begun connecting the dots between positive business growth and the criticality of security. Implementing defensive measures now can help avoid $1MM per day compliance penalties and meet security standards deadlines, from NERC-CIP to IEC 62443-2-4 and ISO27000.

More importantly, strategically aligning the company's security maturity evolution to business growth ensures that cyber disruption is properly accounted for in risk management initiatives.

Defining a security posture baseline

It is important to understand the steps required to implement a security strategy. The easiest way to identify and initiate these steps is to review a security maturity model, with clear actions outlined in a power business environment:

Stage 1 Assess

Identify immediate security issues that can impact operations, even if the environment is thought to be "air gapped." Common findings from expert assessments include unapproved wireless access points or unsafe software—vulnerabilities that attackers can easily exploit. Many immediate issues can be fixed quickly to reduce cyber threat risk.

Stage 2 Protect

Implement security monitoring and defensive layers to comply with standards and strengthen the security posture. Lower the risk of security exploits by using technical solutions, such as purpose-built industrial control security equipment. Set up automation and patch management tools to simplify and expedite security administration. Train teams on what to look for, and how to respond to cyber activities, just as training is mandatory for operations safety.

Stage 3 Prevent

For sophisticated organizations, 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. Regular assessments and security health checks can monitor dynamic environments.

Across all stages, it is critical to maintain a constant vigilance to ensure basic security hygiene is implemented, and cyber security policies are enforced.

Customer spotlight

GE Digital customer:

U.S. plant, combined cycle, with high criticality customer base

Security challenge

Zero visibility into security risk

Solution

OpShield from GE Digital, OT protocol inspection, instrumented in one day

Results

- Avoided NERC CIP v5 compliance violation and associated $1M per day penalty
- Proactively identified diverse security vulnerabilities, including 26 unauthorized hosts
- Gained immediate visibility into control system data communication patterns, helping baseline plant behavior to improve threat discovery

$243 billion—$1 trillion: impact to the U.S. economy of an electricity blackout across 15 U.S. states affecting 93 million people.[4]

GE Digital cyber solutions

GE Digital Power Solutions work at any stage of security maturity to bring greater control, less risk, and increased reliability to a power business. Depending on the situation, there are impactful people, process, and technology actions that can be instituted.

GE Digital's Cyber Solutions include:

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

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 Digital's security experts, who regularly analyze and implement real-world security solutions at operating facilities.

Cyber Asset Protection (CAP)

A security subscription service to centrally deploy, manage, and report on security patches.

CAP automated or scheduled updates help regularly protect critical assets from known vulnerabilities. Additional functionality includes anti-virus/host intrusion detection updates, logging and event management, whitelisting, and automated backup.

SecurityST

A centralized security management solution for turbine, plant, and generator controls environments.

SecurityST provides a single vantage point to see a power company's cyber security posture, implement proactive protection policies, and provide centralized reporting to manage cyber risk. As part of the SecurityST Mark VIe Solution and Commissioning Services, an Achilles™ Practiced Certified—Bronze solution set, Security ST facilitates more efficient compliance to global security standard IEC 62443-2-4.

OpShield

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

OpShield monitors and blocks malicious activity, and minimizes disruptions to enable highly available operations and secure productivity.

Customer benefits

- Reduced risk from cyber attack on key assets, SCADA systems, and operational network infrastructure
- Proactive identification of critical vulnerabilities and security events
- Improved operational reliability and reduced risk in business continuity
- Automated patch management to keep critical systems up to date with latest cyber protection
- Regulatory compliance for NERC CIP, with ability to demonstrate security actions and activities

Customer spotlight

GE Digital customer:

U.S. Power Plant

Security challenge

Air gapped facility with limited visibility of security risk

Solution

Security Health Check

Results

- Availability increased during high revenue pricing of ancillary market operation
- OpShield results prompted plant manager to immediately remediate findings
- Discovered immediate security vulnerabilities: operator control screens running Windows XP OS and outdated versions of HMI software
- Identified security gaps during plant walk through: wireless access point installed in controls environment with no authentication configured

Why cyber security now?

- Unplanned outages/trips cost $96K a day on average (modeled on 500MW block)
- 225,000 people lost power in the Ukraine due to a cyber attack (December 2015)
- NERC CIP v5 carries $1MM per day fine for security compliance violation

$38B in damages from MyDoom virus due to lost productivity, network downtime, and compromised data.[5]

Unplanned disruptions cost 3–8% of capacity, $10B in annual lost production.[6]

Your security partner in the digital industrial world

GE brings over 60 years of experience in developing advanced control systems with detailed knowledge of power environments. Whether retrofitting preexisting environments and equipment, or mapping to new digital power plant footprints, GE Digital security professionals can identify, manage, and reduce cyber risk.

Sources:

[1] *Pew Research Center*

[2] *GE Power*

[3] *Ernst & Young*

[4] *Lloyds Emerging Risk Report, 2015*

[5] *Investopedia, 2012 and PBS Frontline, 2000.*

[6] *GE P&W*

About GE

GE (NYSE: GE) is the world's Digital Industrial Company, transforming industry with software-defined machines and solutions that are connected, responsive, and predictive. GE is organized around a global exchange of knowledge, the "GE Store," through which each business shares and accesses the same technology, markets, structure, and intellect. Each invention further fuels innovation and application across our industrial sectors. With people, services, technology, and scale, GE delivers better outcomes for customers by speaking the language of industry.

Contact Information

Americas: 1-855-YOUR1GE (1-855-968-7143)
gedigital@ge.com

www.ge.com/digital