WURLDTECH SECURITY SERVICES
CYBER RISK BENCHMARK PROGRAM

GE Digital

With the introduction of the Industrial Internet, organizations are increasingly connecting operational technology (OT) to other systems, including a variety of enterprise IT networks. While this new and expanding "cyber meets physical" connectivity promises great rewards – productivity gains, performance optimization and reduced costs – it's not absent of risk.

Industrial control systems (ICS), critical infrastructure and other OT environments must maintain certain levels of availability, productivity, and safety. Any kind of disruption or downtime from a cyber incident – whether malicious or accidental – can be costly on many levels.

Designed to enhance awareness and diminish uncertainty, the Cyber Risk Benchmark Program, delivered in two parts, offers a maturity assessment of your security practices and technologies, uncovers vulnerability across your control systems, and provides insight and guidance on ways to strengthen your overall cybersecurity posture.

APPROACH

PART 1: CYBER MATURITY BASELINE

The Cyber Maturity Baseline begins with a multi-tiered survey across technical, engineering, and executive stakeholders. The survey provides insight into your current security posture based on five core pillars of a successful security strategy:

-Fundamental security management addresses the functions necessary for operation security risk management
-Strategic alignment covers the functions that drive effective OT security risk management
-Infrastructure management meets requirements to ensure effective risk management
-Issue and Incident management relates to the appropriate functions, helps them recover and transfers knowledge
-Governance/Compliance management works with the owners of regulatory, financial and business requirements

Your survey findings portray a snapshot of your security posture, and is rated against both industry standards and peer averages. We also highlight specific areas of concern with recommendations on initial steps to consider.

PART 2: CYBER TECHNOLOGY BASELINE

The baseline is a standardized technical evaluation that examines a specific range of IP addresses in your network. It is designed to show the nature and level of your technology attack surface and address questions such as: What sanctioned and unsanctioned communications are happening on you network?

With this level of information you will be able to make confident decisions with regard to necessary security controls, process changes and governance policies.

DURATION + COST

The Cyber Maturity Baseline takes less than an hour to administer, then two days to synthesize.

The Cyber Technology Baseline can be executed in a day with results coming shortly after completion.

The entire benchmark program is $10,000.