EPRI | ELECTRIC POWER RESEARCH INSTITUTE

EPRI CYBER SECURITY METRICS – A CONTINUOUS PROCESS DRIVING DECISIONS TO REDUCE RISK

The pace-of-change of the cyber threat landscape and increase in cyber security risk for the electric grid require utility companies to continuously improve their security posture through adequate investment in cyber security. Investment in cyber security is however associated with high financial risk because it is difficult to measure the performance of the investment and to quantify exactly how much it improves a company's security posture.

EPRI cyber security metrics is an on-going research project designed to address a gap in security performance measurement. This executive brief provides an overview of the status, progress and next steps for the project. The EPRI security metrics framework leverages OT and IT data generated by cyber security infrastructure to produce a repeatable data-centric process for assessing the performance of cyber security programs. EPRI created sixty metrics that quantify the security performance of an organization. The metrics were categorized into three broad categories each highlighting different aspects of the organization's security posture to diverse stakeholders. EPRI metrics rely on OT and IT data internal to the organization which is a key factor that sets EPRI security metrics apart from other existing security metric systems.

The EPRI security metrics project has been underway for four years. During this time, eight utility companies have pilot tested EPRI security metrics. The results from the pilots has led to significant improvement in metrics calculation methods that have been implemented in EPRI Metrics Version 2. In addition to the pilot tests, a usability survey among pilot test participants was also carried out. The usability survey provided invaluable lessons that have been used to further improve security metrics. The survey was instrumental in identifying the immediate need for tools to simplify the implementation of metrics. Survey participants also indicated the need for more guidance on how to collect data, automate data collection and customize EPRI metrics' software for use with limited data sets. Taking this feedback into account, the EPRI Metrics Framework and tools have been modified and will be evaluated in the next phase of utility pilot projects starting in early 2020.

Goal of EPRI Cyber Security Metrics

The goal of the EPRI security metrics research project is to produce a quantitative, data-driven process for continuously measuring and improving the performance of utilities' cyber security programs in a consistent and repeatable way. The aim is to produce results and data that will enable utilities to make informed decisions on cyber security investments and quantitatively assess their benefit if any. The metrics developed can be applied to both Operations Technology (OT) and Information Technology (IT).

As shown in Figure 1, There are well-established frameworks for cyber security programs, requirements and maturity models, however there is a gap in the industry with regards to measuring the effectiveness of cyber security programs. EPRI security metrics bridge this gap. EPRI metrics quantify the outcome of security programs in place showing how well programs work in protecting from, detecting and responding to cyber-attacks.

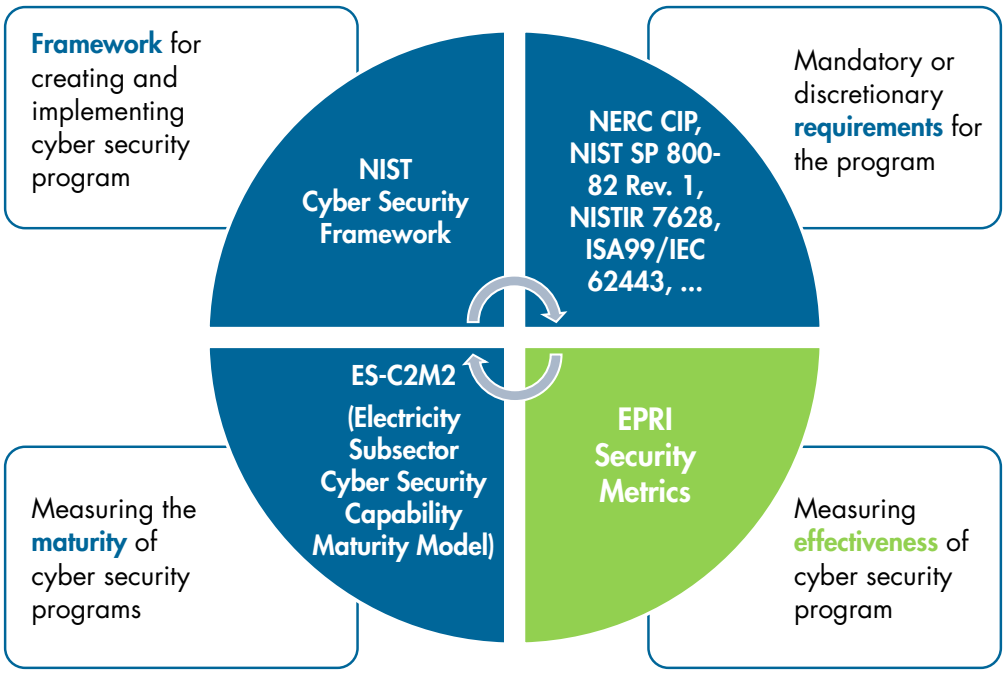

Figure 1. The Role of Security Metrics

EPRI Cyber Security Metrics Overview

EPRI's approach is to organize metrics in a "pyramid," as shown in Figure 2. The data collected from the system (the base of the pyramid) is used to calculate 45 operational metrics. The metrics are then rolled up through a hierarchy, assigned a weight of importance and summarized into tactical, or strategic metrics. **Operational** metrics measure day-to-day operational performance such as time to detect a security event or security event true-positive rate. **Tactical** metrics measure the performance of programs in each domain of security operations. **Strategic** metrics show the overall effectiveness of cyber protection, detection and response programs in the organization.

Strategic metrics present information based upon which business executives, boards and decision-makers can be informed on the three foundational pillars that comprise an organization's security posture namely protection, detection, and response. EPRI security metrics compute a protection score, detection score, and response score. The protection score measures the effectiveness of the organization's protective infrastructure against cyber events while the detection and response scores measure the speed and effectiveness of the organization's cyber event detection and response programs. Strategic metrics are derived from a combination of tactical and operational metrics which are in turn computed from various sources of cyber security data such as CVSS vulnerabilities data and cyber security infrastructure log data.

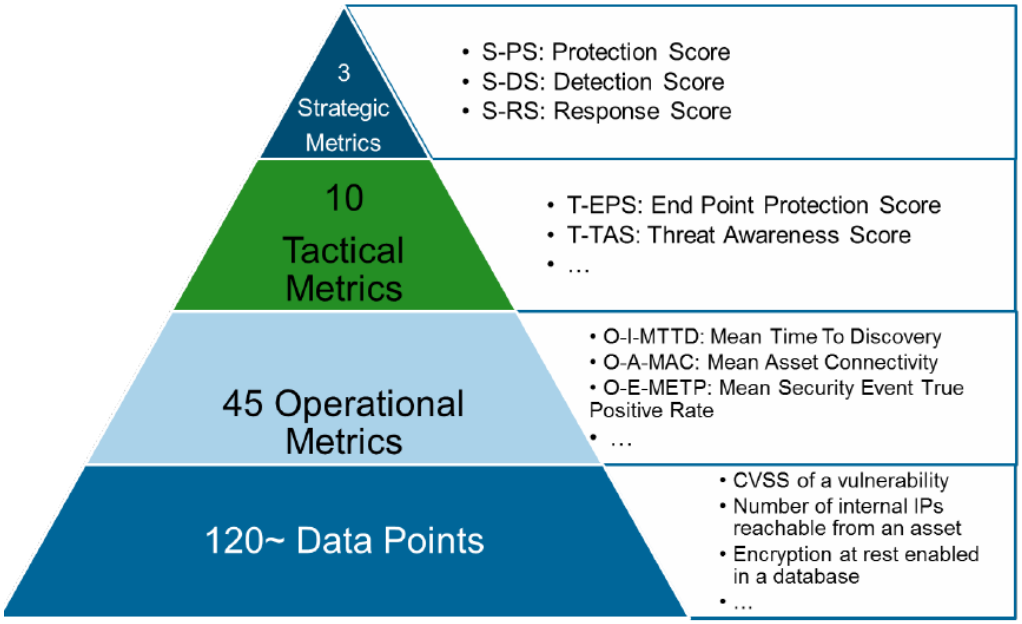

Figure 2. EPRI Cyber Security Metrics Pyramid

EPRI Cyber Security Metrics Examples

The quantitative basis for EPRI security metrics and how they are hierarchically rolled up from low level metrics to high level metrics can be better illustrated by closely examining three operational level metrics-The Mean Time to Recovery (O-I-MTR), Incident Count involving Malicious Email (O-I-ICME) and Mean Human Security Score (O-H-MHSS).

Mean Time to Recovery (O-I-MTR) is an operational metric that measures the average time in days from the day a cyber incident is discovered to the day the incident is completely resolved. The metric uses the data from the incident response records – typically stored in a ticketing system or workforce management system. O-I-MTR contributes to the tactical metric, Incident Response Score (T-IRS) and consequently the strategic metric **Response Score (S-RS)**

Incident Count involving Malicious Email (O-I-ICME) is computed from the number of all cyber incidents in a given period and the number of cyber incidents involving malicious email reported by security systems. O-I-ICME in one contributing metric to the tactical metric, Perimeter Protection Score (T-PPS), which in turn contributes to the strategic metric, **Protection Score (S-PS)**.

Mean Human Security Score (O-H-MHSS) measures the human factor in cyber security operations. O-H-MHSS calculated from 7 data points from Incident records, security training records, and logical/physical access lists. It is rolled up to the tactical metric, Human Security Score (T-HSS) and the strategic metric, **Protection Score (S-PS)**.

EPRI Cyber Security Metrics Attributes

Cyber risk assessment platforms that include quantitative metrics are becoming gradually adopted in the industry with key players including companies like Bitsight, MetricStream, RSA and Up guard. However, these risk assessment platforms predominantly focus on IT systems and tend to provide insights into risks that are externally visible and common to multiple organization. There two key factors that differentiate EPRI security metrics.

First, EPRI security metrics provide a comprehensive view of the performance of an organization's security operation covering all three areas of cyber security; protection, detection and response. Other frameworks on the other hand focus on one or two specific aspects of cyber security (for example patch management of external-facing systems)

Secondly, EPRI metrics have been developed and tested with data from industrial control systems uniquely qualifying them to provide the OT perspective for utility security operations. While EPRI metrics can also be applied to IT-systems the overall results provide insight into OT security operations better than other generic metrics systems.

Key Findings and Lessons Learned from the 8 EPRI Metrics Pilots

EPRI started its cyber security metrics research project in 2015 and has since engaged domestic and international utilities leading to a series of 8 utility pilot projects and a usability survey in 2018. The 2018 pilot tests and usability survey resulted in some key findings that have been instrumental to the improvements that led to EPRI Metrics Version 2.

The studies conducted highlighted the feasibility and value of EPRI security metrics. The metrics provide comprehensive insights enveloping the three main pillars of any organization's cyber security posture by computing a protection score, a detection score and a response score. Additionally, participants of the study agreed that EPRI security metrics were data-driven in nature, making them objective, consistent and possible to automate. Finally, the three tiers categorizing the metrics into strategic, tactical or operational levels made EPRI metrics easy to understand by the stakeholders according to the usability survey.

The results also showed a few opportunities for improvement. The most prominent ones were with respect to the time and efforts required for data collection and the need for standardization and benchmarking.

What's Next? EPRI Metrics Operationalization and Benchmarking Pilot – Phase 2

The lessons learned from the pilot study were used to formulate the key areas of focus for 2019 and beyond. The current focus of the EPRI security metrics project is to improve usability by developing tools and training materials.

To facilitate data collection and metrics calculation, EPRI developed a software tool called MetCalc—The EPRI Metrics Calculator. MetCalc supports utilities that seek to use the EPRI cyber security metrics in their environment with functionality to:

- Load data
- Modify various factors for each metric, if required
- Generate a dashboard
- Export the project data into Microsoft Excel format
- Set target values for each metric
- Load industry reference values for comparison

The 2018 pilot tests and usability survey led to significant improvement of EPRI security metrics and the creation of tools to support the use of metrics. A pilot project seeking to operationalize and benchmark updated security metrics is currently underway. The EPRI metrics operationalization and benchmarking pilot project will facilitate:

- Customization of MetCalc
- Automation of the data collection
- Metrics benchmarking
- Advanced analytics for improving security posture
- Process development and training

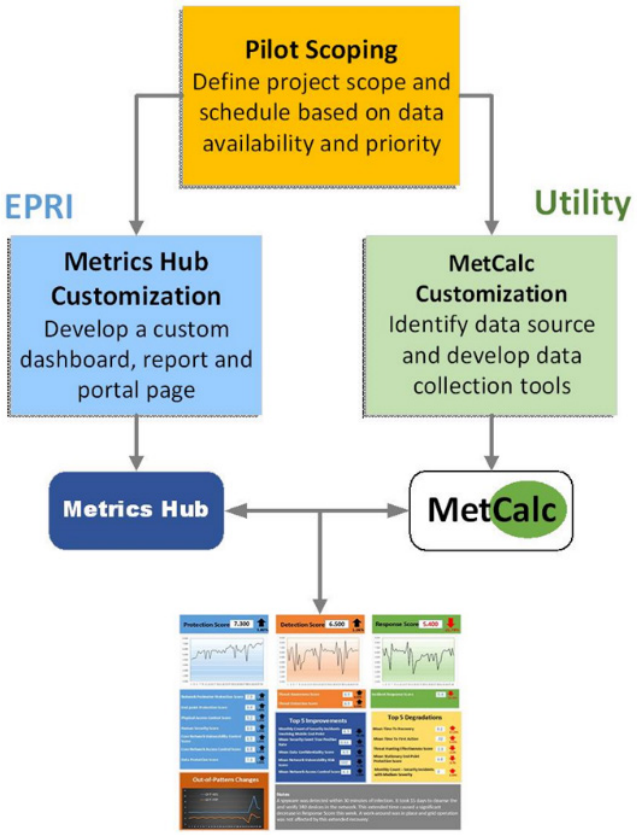

Figure 3. Metrics Operationalization and Benchmarking

Key Benefits for Participating Utilities

The value of the knowledge attained and tools developed from EPRI's four-year research on cyber security metrics will be transferred to member utility companies. The pilot project has been created to enable participating utilities to customize and implement EPRI security metrics to measure the performance of their security investments with the aim of improving cyber security operations. The data-driven nature of the security metrics will also provide objective and reliable information based upon which decision-makers can adequately allocate resources.

More information on EPRI Cyber Security Metrics Operationalization and Benchmarking Pilot can be downloaded from epri.com.

Beyond 2020—The Roadmap for EPRI Metrics

Figure 4 shows the roadmap for EPRI security metrics project. Since its inception in 2015, the EPRI cyber security metrics research project has undergone several stages each accomplishing a set of goals. The EPRI security metrics project is presently at Stage 3 focusing on interoperability, specification and adoption support. During this stage, beta versions of Metrics Hub and MetCalc tools are released to the public. Stage 3 will also see the formation of the metrics advisory council (MAC) to provide technical expertise and advice on the adoption and interoperability of EPRI metrics for utility vendors. The EPRI metrics project will conclude with Stage 4 that is envisioned to produce sharable playbooks and implementation guides, enabling data-driven, evidence-based decision making for cyber security.

Figure 4. EPRI Security Metrics for the Electric Sector Roadmap

Technical Contact

Candace Suh-Lee
Principal Project Manager – Cyber Security, PDU
650.855.8513, csuh-lee@epri.com

The Electric Power Research Institute, Inc. (EPRI, www.epri.com) conducts research and development relating to the generation, delivery and use of electricity for the benefit of the public. An independent, nonprofit organization, EPRI brings together its scientists and engineers as well as experts from academia and industry to help address challenges in electricity, including reliability, efficiency, affordability, health, safety and the environment. EPRI also provides technology, policy and economic analyses to drive long-range research and development planning, and supports research in emerging technologies. EPRI members represent 90% of the electricity generated and delivered in the United States with international participation extending to 40 countries. EPRI's principal offices and laboratories are located in Palo Alto, Calif.; Charlotte, N.C.; Knoxville, Tenn.; Dallas, Texas; Lenox, Mass.; and Washington, D.C.

Together . . . Shaping the Future of Electricity

3002017501 October 2019

Electric Power Research Institute
3420 Hillview Avenue, Palo Alto, California 94304-1338 • PO Box 10412, Palo Alto, California 94303-0813 USA • 800.313.3774
• 650.855.2121 • askepri@epri.com • www.epri.com

© 2019 Electric Power Research Institute (EPRI), Inc. All rights reserved. Electric Power Research Institute, EPRI, and TOGETHER . . . SHAPING THE FUTURE OF ELECTRICITY are registered service marks of the Electric Power Research Institute, Inc.