EPRI | ELECTRIC POWER RESEARCH INSTITUTE

Cyber Security Metrics for the Electric Sector

Volume 4

3002013690

Cyber Security Metrics for the Electric Sector

Volume 4

3002013690

Technical Update, December 2018

EPRI Project Manager

C. Suh-Lee

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

DISCLAIMER OF WARRANTIES AND LIMITATION OF LIABILITIES

This is an EPRI Technical Update report. A Technical Update report is intended as an informal report of continuing research, a meeting, or a topical study. It is not a final EPRI technical report.

NOTE

For further information about EPRI, call the EPRI Customer Assistance Center at 800.313.3774 or e-mail askepri@epri.com.

ACKNOWLEDGMENTS

The Electric Power Research Institute (EPRI) prepared this report:

Principal Investigator
C. Suh-Lee

Contributor
A. Avadhanula

This report describes research sponsored by EPRI.

This publication is a corporate document that should be cited in the literature in the following manner:

Cyber Security Metrics for the Electric Sector: Volume 4. EPRI, Palo Alto, CA: 2018. 3002013690.

ABSTRACT

Cyber security metrics for the electric sector is an ongoing research project that EPRI is leading in collaboration with multiple North American utility companies. The project focuses on developing, testing, and refining a set of metrics to quantify the effectiveness of cyber security controls. Once operationalized, the metrics can provide meaningful, scientific cyber security information to various stakeholders. EPRI has pilot tested a total of 60 metrics calculated from 120–150 data points using real-world data collected from many EPRI member utilities. While these data are analyzed for further improvement of EPRI metrics, the project has also conducted a usability survey among a few utility members that have been following this research closely. This report includes the key statistics from the metric pilot and discuss the results of the usability survey.

Keywords
Cyber security
Cyber security metrics
Cyber security performance metrics
Cyber security risk management
Cyber security metric calculator
Information assurance

Deliverable Number: 3002013690

Product Type: Technical Update

Product Title: Cyber Security Metrics for the Electric Sector: Volume 4

PRIMARY AUDIENCE: Utility cyber security management, cyber security architect, security operation center personnel, security engineer, risk manager

SECONDARY AUDIENCE: Utility chief information officer, chief information security officer, chief technology officer, vice-president of operations

KEY RESEARCH QUESTION

This research seeks to determine the level of ease or difficulty in using EPRI metrics in utilities' cyber security operations, identify the primary difficulties in operationalizing EPRI cyber security metrics, and determine utility readiness to operationalize the metrics.

RESEARCH OVERVIEW

Cyber security metrics for the electric sector is an ongoing research project that EPRI is leading in collaboration with multiple North American utility companies. The project focuses on developing, testing, and refining a practical method to quantify the effectiveness of cyber security controls and to accumulate the quantified data over a period to provide meaningful, scientific cyber security information to various stakeholders. The project team has pilot tested a total of 60 metrics, calculated from 120–150 data points, using real-world data collected from EPRI member utilities. By analyzing this data gathered through the pilot exercise, the study plans to produce a common set of cyber security metrics, which can be used for industry-level benchmarking, as well as to identify ways to enhance the cyber security posture of participating utilities.

KEY FINDINGS

- Preliminary statistics from the pilot study show interesting insights for EPRI metrics, their effectiveness, and usage examples.
- The metrics usability survey suggests that EPRI metrics are easy to understand when presented, but are difficult to explain to a stakeholder.
- Sixty-one percent of survey respondents said they would start collecting the data to use EPRI metrics within one year, if they have useful guidelines and tools. Twenty-eight percent of respondents said they would start right away, with the guidelines and tools.
- Seventy-six percent of respondents indicated that "data collection guidelines including information on data sources and existing tools" is the most helpful factor for metric operationalization.
- In the future, the project will focus on operationalization support, such as producing guidelines, training materials, and necessary tools.

WHY THIS MATTERS

The changing threat landscapes and increasing cyber security risks on the electric grid require utilities to continuously improve their security postures through adequate investment in cyber security. However, investment in cyber security is generally considered to carry relatively high financial risk, because of the difficulty of quantifying the cyber security risk reduction and attributing it to certain investments. By measuring the effectiveness of cyber security controls in a consistent way using EPRI metrics, a utility can objectively estimate the value of the cyber security investment.

HOW TO APPLY RESULTS

This research provides a set of comprehensive cyber security metrics for utility implementation. Once operationalized, the metrics provide a quantitative way to measure the value of investment in security technology, processes, or people. However, to fully realize the value of the standard metrics, some form of industry-level collaboration to produce statistics for benchmarking is needed. When this industry collaboration matures, cyber security metrics may be communicated in a manner similar to how reliability and safety indices are reported throughout business units.

LEARNING AND ENGAGEMENT OPPORTUNITIES

EPRI has developed the following background materials:

- *Cyber Security Metrics for the Electric Sector, Volume 3.0*. EPRI, Palo Alto, CA: 2016. 3002010426
- *Creating Security Metrics for the Electric Sector, Version 2.0*. EPRI, Palo Alto, CA: 2016. 3002007886.
- *Creating Security Metrics for the Electric Sector. EPRI, Palo Alto, CA*: 2015. 3002005947.

EPRI CONTACTS: Candace Suh-Lee, Principal Technical Leader, csuh-lee@epri.com

PROGRAM: P183 – Cyber Security

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

ACRONYMS

CIP	Critical infrastructure protection
CSF	Cyber security framework
C2M2	Cybersecurity capability maturity model
EPRI	Electric Power Research Institute
IT	Information technology
OT	Operations technology
MetCalc	Security metric calculator
NERC	North American Electric Reliability Corporation
NIST	National Institute of Standards and Testing
NISTIR	NIST Internal/Interagency Reports
SCADA	Supervisory control and data acquisition
SME	Subject matter expert

CONTENTS

LIST OF FIGURES

LIST OF TABLES

1
INTRODUCTION

Cyber security metrics for the electric sector is an ongoing research project that EPRI is leading in collaboration with multiple North American utility companies. The project focuses on developing, testing, and refining a practical method to quantify the effectiveness of cyber security controls and to accumulate the quantified data over a period to provide meaningful, scientific cyber security information to various stakeholders. In past years, the project team has pilot tested a total of 60 metrics, calculated from 120–150 data points, using real-world data collected from EPRI member utilities. In 2018, the project focused on analyzing this data gathered through the pilot exercise to enhance the metrics so they can better reflect cyber security operations in the real world.

Project Approach

EPRI's approach, as shown in the metrics "pyramid" (see Figure 1-1), organizes data points, then rolls them up through a metrics hierarchy and assigns a weight of importance to each operational, tactical, or strategic metric. The resulting tiers of data help a broad range of utility stakeholders gain improved knowledge about cyber security postures, and thus inform decision-making about policies, investments, and action plans.

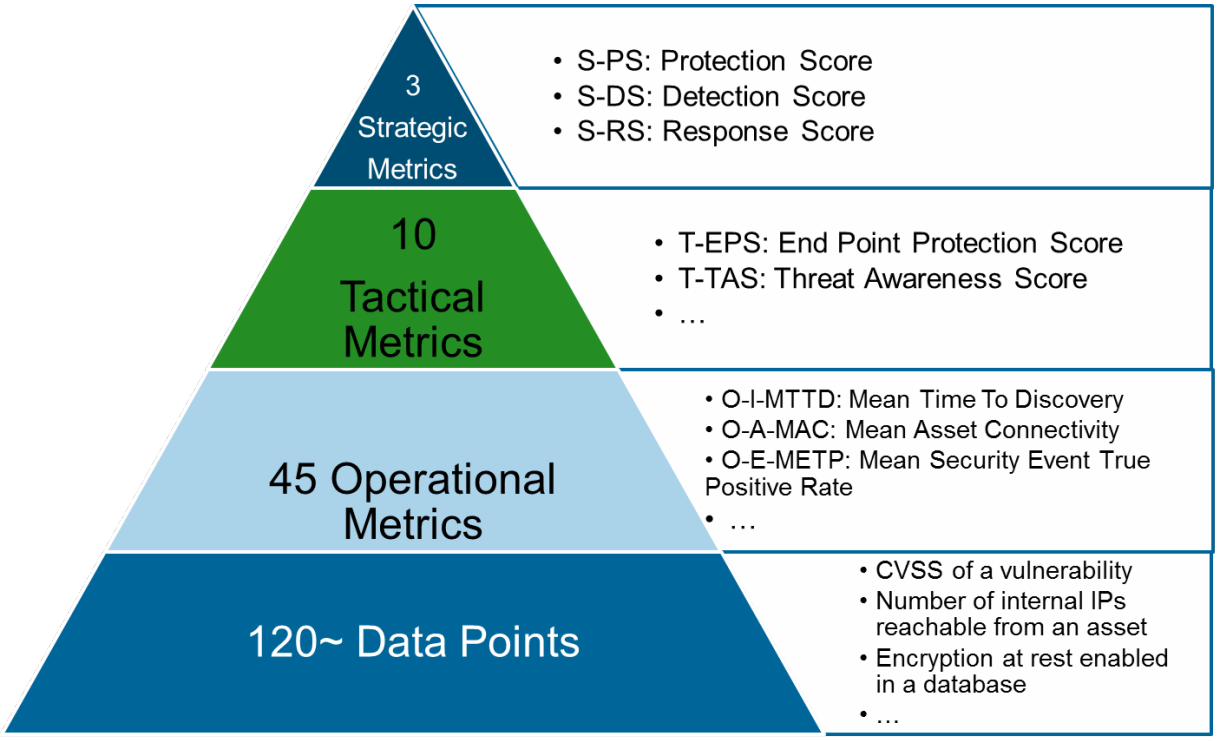

Figure 1-1
EPRI cyber security metrics pyramid

Approximately 120-150 data points provide the quantitative foundation for the metrics, consisting of various operational statistics collected from various points in utility operations. The availability and quality of these data are important factors in metrics calculations.

Operational metrics measure real-time, day-to-day operations such as logs, rule sets, and signatures. Tactical metrics address programmatic health and progress in the organization. Strategic metrics measure corporate risk and alignment of the metrics in the direction of the business.

Metrics to Enhance Cyber Security

A cyber security metrics program can help improve utility cyber security programs by:

- Providing quantifiable information about cyber security to support enterprise risk management decisions in a similar way to financial, reliability, and other business-driven risk discussions
- Articulating and tracking progress towards goals using a repeatable method
- Increasing accountability for cyber security by identifying gaps or ineffective security practices that need to be addressed
- Providing an objective context to compare and benchmark cybersecurity-related practices across organizations and information technology/operations technology (IT/OT) environments

Utilities can use the results of the metrics calculations to continually improve their cyber security program. Figure 1-2 illustrates the various cyber security frameworks and standards available for the electric sector and the role of cyber security metrics in overall information assurance and cyber security governance:

- The National Institute of Standards and Testing (NIST) cyber security framework (CSF) helps utilities identify the key components of a cyber security program and organize utility programs [3].
- NERC CIP [4], NIST SP 800 series, and NISTIR 7628 [6] are mandatory or discretionary requirements that apply to the utility's cyber security program.
- The Cybersecurity Capability Maturity Model (C2M2) – a public-private partnership that the U.S. Department of Energy leads – measures the maturity of the *overall* cyber security program [7].
- The missing piece of the puzzle, addressed in this EPRI cyber security metrics research project, is a way to measure *specific* results of the cyber security program and hence identify ways to improve the cyber security program.

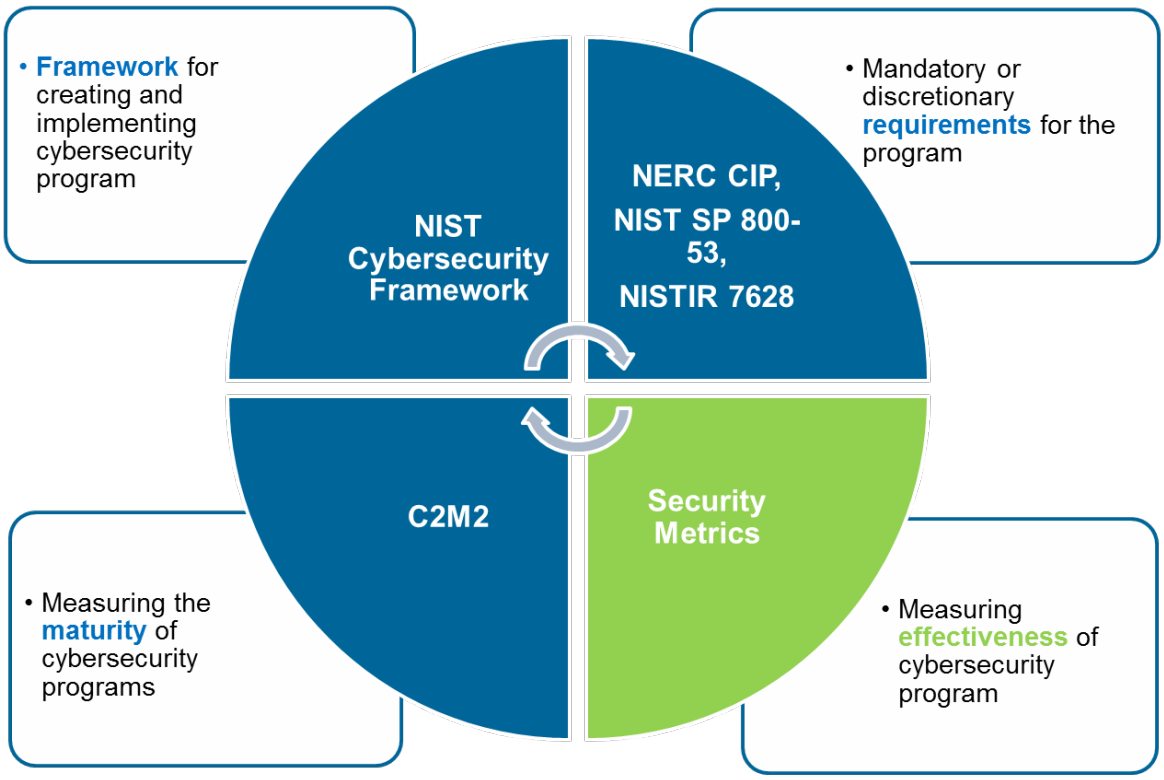

Figure 1-2
Role of security metrics in a cyber security program

Project Work to Date

Figure 1-3 shows the overall flow of the EPRI cyber security metrics projects over time. EPRI has achieved significant progress in this research project, prior to the pilot testing phase. In December 2015, EPRI published a Technical Update entitled "Creating Security Metrics for the Electric Sector" [1]. This report documented the following:

- The conceptual use of cyber security metrics in improving security risk management.
- Discussion of strategic, tactical, and operational level measurements.
- Use of security standards and guidelines as inputs for security metrics.
- The leveraging of existing security maturity models to help formulate a more comprehensive security metrics program.
- Sample metric samples/templates modified for electric power sector use.
- Implementing a security metrics program with a process goal of continual improvement.
- A detailed description of a sample electric power industry-specific security metric.

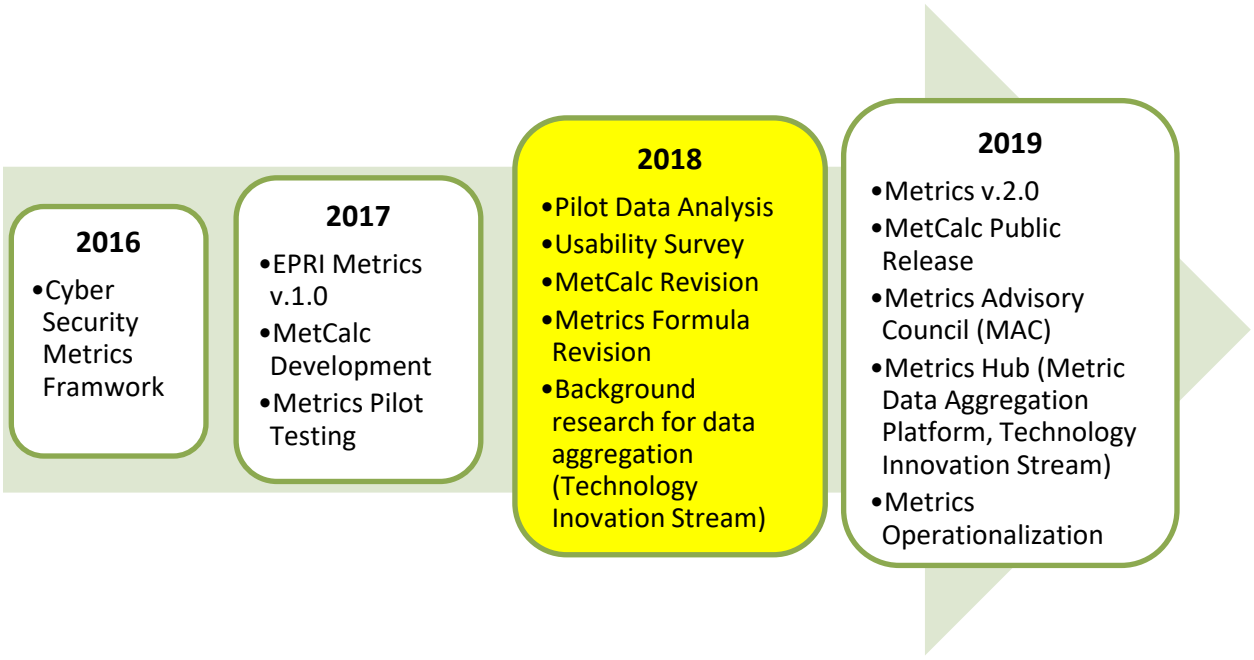

Figure 1-3
EPRI cyber security metrics project progress and future plan

In 2016, EPRI published a Technical Update entitled "Creating Security Metrics for the Electric Sector, Version 2.0" [2]. This report described the following:

- A structure for formulating a cyber security program, incorporating mandatory and discretionary requirements (regulatory), measuring the effectiveness of the program (cyber security metrics), and assessing the maturity of the program over time.
- Guidance on evaluating security program goals and capabilities.
- Expanding/incorporating existing metrics and risk management efforts
- Sixty proposed metrics and 121 data points as the bases for the metric calculation

In 2017, EPRI advanced this project and published a Technical Update entitled "Cyber Security Metrics for the Electric Sector, Volume 3.0." This report includes the following:

- The base formulae for EPRI's 60 cyber security metrics.
- Pilot testing of metrics with the help of the MetCalc (Security Metric Calculator) tool.
- Background on EPRI metrics, how they can be used to calculate security metrics based on a set of data, and how the factors can be adjusted to fine tune the metric value to fit a specific utility environment.
- Various techniques used in metrics calculations, including numerical value, ratio assignment, scoring functions, and aggregations methods.
- Characteristics of metrics, such as flexibility, comparability, and quality of data.
- Complete information on data points required to calculate EPRI's cyber security metrics.

In 2018, EPRI continued to make progress with the project. This includes the following accomplishments:

- The team continued pilot testing of the security metrics using the MetCalc tool at volunteer utilities. The member utilities participating in the metrics pilot program tested the metrics using data from their IT/OT environments and provided feedback on the accuracy, usability, and utility of the metrics.
- The metrics formulae were enhanced based on pilot data analysis. EPRI Cyber Security Metrics Version.2.0 is scheduled to be released in 2019.
- The MetCalc tool is being enhanced, including and improved user interface and additional dashboard with graphical representations to view strategic, tactical, and operational metrics scores.
- The team conducted a usability survey to identify the best ways to support operationalization of the EPRI metrics.

The research will continue throughout the execution of this multi-year project with guidance from advisors of member utilities.

Organization of this Report

Section 2 of this report provides an overview of the pilot testing process and preliminary results from the pilot data analysis.

Section 3 introduces functions for the improved MetCalc tool.

Section 4 discusses the results of the metric usability survey.

Section 5 describes the next steps for this project and related research activities.

Section 6 provides references.

2
METRICS PILOT AND DATA ANALYSIS

Pilot Testing with Utilities

Cyber security metrics need to accurately reflect real-world security operations. This is the primary motivation for the pilot testing phase of this project. During the pilot testing, subject matter experts (SMEs) from the participating utility sample a portion of their system, collect data from the sampled system for a fixed period, load the collected data to the EPRI Cyber Security Metrics Calculator (MetCalc), and calculate the 60 security metrics representing three areas of cyber security: protection, detection, and response.

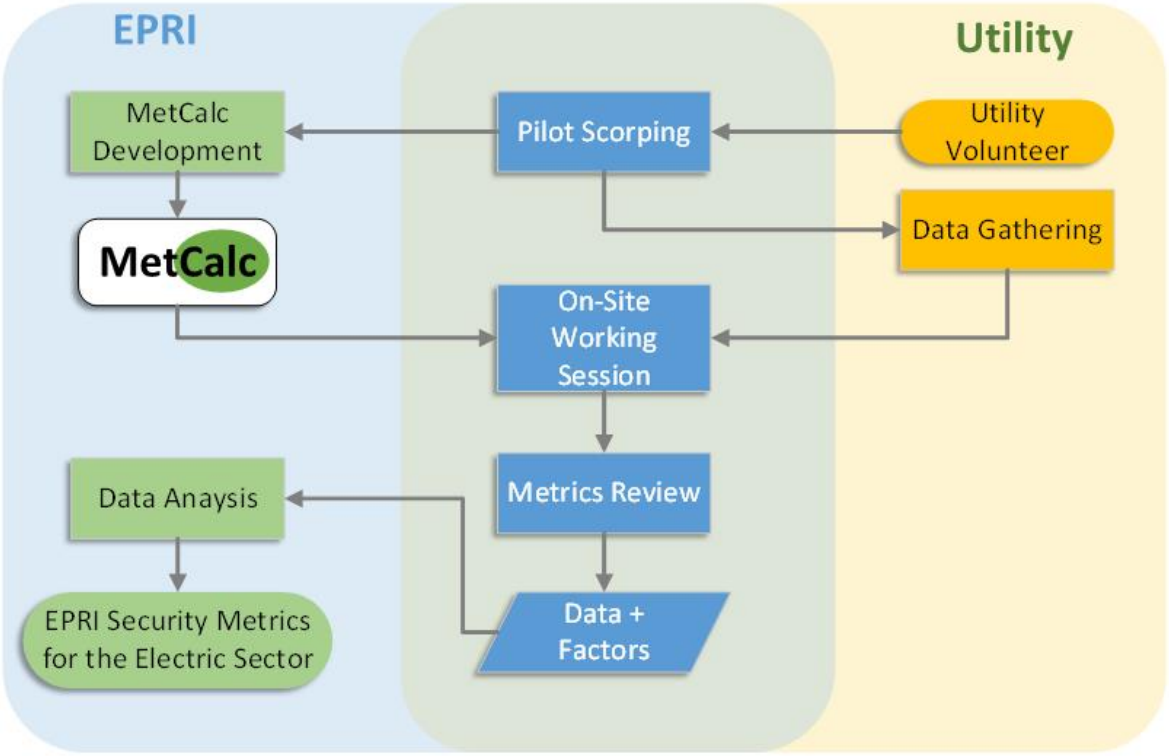

Figure 2-1
Workflow for cyber security metrics pilot testing

The participating utilities and EPRI worked closely to ensure that the calculated metrics reflect the actual security status of sampled systems. Once the 60 metrics were successfully calculated and tuned, the project team conducted a metrics review session with the various stakeholders within the company to review the calculated metrics. The utility review sessions typically led to in-depth discussions of the validity of the metric values, the effectiveness of current security controls, and the plan for improvement in areas where the metrics showed lower than expected values (see Figure 2-1).

Participant data privacy and anonymity are an integral part of the pilot data gathering and analysis process. Therefore, EPRI and the participating utilities used a process for masking data origination and securely collecting data using strong encryption to and from participant sites and EPRI offices.

EPRI is currently analyzing the data gathered through this collaboration to improve the security metrics.

Preliminary Results from Metric Data Analysis

The tables in this section summarize the statistics from the metric pilot study. Data collected are divided by monthly data sets and processed for metric calculation. Calculated metrics are examined for error and compiled to produce the statistics in this section.

The following selected statistics are reported:

- Min – minimum observed value
- Max – maximum observed value
- Count – the number of data sets with a valid metric value
- Mean – arithmetic average of all valid values
- Median – middle value
- Mode – most frequent value

Any number that cannot be calculated due to a data limitation is shown as "NA."

Note for Interpretation or Comparison of Metric Values

EPRI metric values can be meaningfully compared among different datasets as long as the values are for the same metric. For example, if metric K was 5.0 one month ago and has a value 6.5 this month, a reliable conclusion is that the security controls and activities associated with metric K have performed better in the current month than the previous month. However, the values cannot be compared across different metrics, since the score does not indicate the effectiveness in an absolute sense. For example, if metric K is 5.0 and metric L for the same data set is 8.0, this does NOT mean the security controls associated with metric L is more effective than those of metric K. To be meaningful, a value for metric K must be compared with another value for the same metric K -- either from another dataset from a different time period, or from All values reported in this report are preliminary at this time. Some factors that significantly affect metric values, such as weights for each metric, are still being studied. The pilot sampling was conducted based on the availability of data, time, and resources. Moreover, the sample size and data collection process do not guarantee any statistical significance to the collected sample. Therefore, these results should be considered as a set of examples to aid understanding of the EPRI metrics and should not be interpreted as an indicator of the security posture of a company, a group of companies, or the industry.

Strategic Metrics

Three strategic metric scores are shown in Table 2-1. (Strategic metrics are indicated with an "S" at the beginning of the metric ID.) The Detection Score is generally lower than other strategic metrics across all data sets. The difference seems to be related to how the metrics are calculated

(i.e., metric formulae), rather than the effectiveness of security controls indicated by the data. The project team is currently examining various options to improve this seemingly inaccurate representation.

Table 2-1
Strategic metric scores

Metric ID	Metric Name	Min	Max	Count	Mean	Median	Mode	STD
S-PS	Protection Score	5.625	9.270	14	8.162	8.900	8.900	1.244
S-DS	Detection Score	3.300	8.700	11	6.170	6.580	6.120	2.657
S-RS	Response Score	6.650	9.990	9	8.616	9.009	NA	1.261

Tactical Metrics

Ten tactical metric values are shown in Table 2-2. (Tactical metrics are indicated with a "T" at the beginning of the metric ID.) The metrics are organized by the strategic metric categories.

Table 2-2
Tactical metric scores by the strategic metric

Metric ID	Metric Name	Min	Max	Count	Mean	Median	Mode	STD
S-PS	**Protection Score**	**5.625**	**9.270**	**14**	**8.162**	**8.900**	**8.900**	**1.244**
T-NPPS	Network Perimeter Protection Score	4.970	10.000	14	8.935	9.790	10.000	1.525
T-EPS	End-point Protection Score	3.584	9.889	11	8.165	9.111	NA	2.137
T-PAS	Physical Access Control Score	4.166	10.000	11	8.518	10.000	10.000	2.548
T-HSS	Human Security Score	3.254	5.840	11	4.875	5.000	5.000	0.664
T-NVS	Core Network Vulnerability Control Score	4.510	10.000	11	8.967	10.000	10.000	1.924
T-NAS	Core Network Access Control Score	5.382	10.000	11	8.873	10.000	10.000	1.945
T-DPS	Data Protection Score	5.467	10.000	10	9.187	10.000	10.000	1.729
S-DS	**Detection Score**	**3.300**	**8.700**	**10**	**6.786**	**7.189**	**6.120**	**1.786**
T-TAS	Threat Awareness Score	3.670	6.769	10	5.201	4.603	4.230	1.343
T-TDS	Threat Detection Score	3.094	9.530	10	7.420	7.775	6.870	2.073
S-RS	**Response Score**	**6.650**	**9.990**	**9**	**8.616**	**9.009**	**NA**	**1.261**
T-IRS	Incident Response Score	6.650	9.990	9	8.616	9.009	NA	1.261

Operational Metrics

Tables 2.3-2.14 show the metric values from the pilot study for all operational metrics. (Operational metrics are indicated with an "O" at the beginning of the metric ID.) The metrics are organized by the tactical metric categories.

Table 2-3
Operational Metrics for T-NPPS

Metric ID	Metric Name	Min	Max	Count	Mean	Median	Mode	STD
T-NPPS	**Network Perimeter Protection Score**	**4.970**	**10.000**	**14**	**8.935**	**9.790**	**10.000**	**1.525**
O-N-MAPS	Mean Access Point Protection Score	0.899	9.940	6	6.972	7.885	7.890	3.109
O-N-MWAPS	Mean Wireless Access Point Protection Score	0.000	9.890	2	4.945	4.945	NA	6.993
O-N-MIPS	Mean Internet Traffic Protection Score	7.634	7.634	1	7.634	7.634	NA	NA
O-I-ICME	Mean Count-M Malicious Email	0.000	3.000	9	0.778	0.000	0.000	1.093
O-I-ICMU	Mean Count-M Malicious URL	0.000	3.000	9	0.333	0.000	0.000	1.000
O-I-ICNP	Mean Count-M Network Penetration	0.000	0.000	9	0.000	0.000	0.000	0.000

Table 2-4
Operational metrics for T-EPS

Metric ID	Metric Name	Min	Max	Count	Mean	Median	Mode	STD
T-EPS	**End-point Protection Score**	**3.584**	**9.889**	**11**	**8.165**	**9.111**	**NA**	**2.137**
O-U-MSDPS	Mean Stationary End-Point Protection Score	0.000	8.730	3	4.365	4.365	NA	6.173
O-U-MMDPS	Mean Mobile End-Point Protection Score	2.560	8.917	3	4.936	3.331	NA	3.469
O-I-ICMW	Mean Count-M Malware	0.000	7.000	9	2.111	1.000	0.000	2.571
O-I-ICMD	Mean Count-M Mobile End-Point	0.000	9.000	9	2.222	1.000	3.000	2.863
O-I-ICSD	Mean Count-M Stationary End-Point	0.000	10.000	9	4.444	4.000	4.000	3.167

Table 2-5
Operational Metrics for T-PAS

Metric ID	Metric Name	Min	Max	Count	Mean	Median	Mode	STD
T-PAS	**Physical Access Control Score**	**4.166**	**10.000**	**11**	**8.518**	**10.000**	**10.000**	**2.548**
O-A-MPACS	Mean Physical Access Control Score	0.499	5.130	3	3.343	4.400	NA	2.490
O-I-MPAV	Monthly Incident Count - Physical Access Violation	0.000	1.000	9	0.111	0.000	0.000	0.333

Table 2-6
Operational metrics for T-HSS

Metric ID	Metric Name	Min	Max	Count	Mean	Median	Mode	STD
T-HSS	**Human Security Score**	**3.254**	**5.840**	**11**	**4.875**	**5.000**	**5.000**	**0.664**
O-H-MHSS	Mean Human Security Score	2.683	5.840	3	3.926	3.254	NA	1.682
O-I-ICSE	Mean Count-M Social Engineering	0.000	2.000	9	0.444	0.000	0.000	0.726
O-I-CNSR	Monthly Incident Count – Non-Security Staff Reporting	0.000	3.000	9	0.667	0.000	0.000	1.000

Table 2-7
Operational metrics for T-NVS

Metric ID	Metric Name	Min	Max	Count	Mean	Median	Mode	STD
T-NVS	**Core Network Vulnerability Control Score**	**4.510**	**10.000**	**11**	**8.967**	**10.000**	**10.000**	**1.924**
O-A-MAC	Mean Asset Connectivity	7.020	10.000	3	8.735	9.184	NA	1.540
O-A-MAP	Mean Asset Proximity from a Hostile Network	3.940	8.367	2	6.154	6.154	NA	3.130
O-A-MVRS	Mean Asset Vulnerability Risk Score	1.923	1.923	1	1.923	1.923	NA	NA
O-A-MNVRS	Mean Network Vulnerability Risk Score	0.530	3.985	2	2.258	2.258	NA	2.443
O-I-ICNP	Mean Count-M Network Penetration	0.000	0.000	9	0.000	0.000	0.000	0.000

Table 2-8
Operational metrics for T-NAS

Metric ID	Metric Name	Min	Max	Count	Mean	Median	Mode	STD
T-NAS	**Core Network Access Control Score**	**5.382**	**10.000**	**11**	**8.873**	**10.000**	**10.000**	**1.945**
O-A-MAC	Mean Asset Connectivity	7.030	10.000	3	8.738	9.184	NA	1.534
O-A-MAP	Mean Asset Proximity To Hostile Network	3.940	8.367	2	6.154	6.154	NA	3.130
O-A-MACS	Mean Asset Access Control Score	4.887	9.974	3	7.870	8.750	NA	2.655
O-A-MNACS	Mean Network Access Control Score	2.277	4.987	3	3.348	2.780	NA	1.441
O-I-ICNP	Mean Count-M Network Penetration	0.000	0.000	9	0.000	0.000	0.000	0.000

Table 2-9
Operational metrics for T-DPS

Metric ID	Metric Name	Min	Max	Count	Mean	Median	Mode	STD
T-DPS	**Data Protection Score**	**5.467**	**10.000**	**10**	**9.187**	**10.000**	**10.000**	**1.729**
O-D-MDCS	Mean Data Confidentiality Score	5.200	8.467	2	6.834	6.834	NA	2.310
O-D-MDIS	Mean Data Integrity Score	1.000	6.600	2	3.800	3.800	NA	3.960
O-D-MDAS	Mean Data Availability Score	4.666	7.410	2	6.038	6.038	NA	1.940
O-I-MCDL	Mean Count-M Data Leak/Loss	0.000	0.000	9	0.000	0.000	0.000	0.000

Table 2-10
Operational metrics for T-TAS

Metric ID	Metric Name	Min	Max	Count	Mean	Median	Mode	STD
T-TAS	**Threat Awareness Score**	**3.670**	**6.769**	**10**	**5.201**	**4.603**	**4.230**	**1.343**
O-T-TIES	Threat Intelligence Effectiveness Score	1.000	5.655	10	3.443	3.038	2.160	1.901
O-T-MTIA	Mean Time from Intelligence to Action	0.000	1.000	9	0.148	0.000	0.000	0.338
O-T-MTIP	Mean Time from Intelligence to Protection	0.000	4.750	9	1.140	0.667	0.000	1.670
O-T-THES	Threat Hunting Effectiveness Score	0.000	5.156	10	2.902	3.513	5.156	2.424

Table 2-11
Operational metrics for T-TDS

Metric ID	Metric Name	Min	Max	Count	Mean	Median	Mode	STD
T-TDS	**Threat Detection Score**	**3.094**	**9.530**	**10**	**7.420**	**7.775**	**6.870**	**2.073**
O-T-TIAR	Mean Threat Intelligence True Positive Rate	0.000	1.000	9	0.525	0.833	0.000	0.501
O-E-METP	Mean Security Event True Positive Rate	0.001	0.800	9	0.111	0.024	NA	0.259
O-T-THTP	Mean Threat Hunting True Positive Rate	0.000	0.000	4	0.000	0.000	0.000	0.000
O-I-MTTD	Mean Time to Discovery	0.000	9.300	9	1.033	0.000	0.000	3.100
O-I-CMISS	Monthly Count-M Missed Security Incidents	0.000	10.000	9	1.444	0.000	0.000	3.245
O-I-CIH	Mean Count-M High Severity	0.000	1.000	9	0.111	0.000	0.000	0.333

Table 2-12
Operational metrics for T-EPS

Metric ID	Metric Name	Min	Max	Count	Mean	Median	Mode	STD
T-IRS	**Incident Response Score**	**6.650**	**9.990**	**9**	**8.616**	**9.009**	**NA**	**1.261**
O-I-MTTC	Mean Time to Containment	0.000	31.500	9	6.856	4.400	0.000	9.879
O-I-MTTR	Mean Time to Recovery	0.000	52.750	9	17.255	14.270	NA	16.848
O-I-MTTA	Mean Time to First Action	0.000	9.000	9	3.670	2.400	0.000	3.535
O-I-MCRM	Mean Cost of Response in Man-Hour (existing resource)	1.000	32.500	6	9.327	4.856	NA	11.723
O-I-MCRX	Mean Cost of Response in Dollar Amount (extra resource)	0.000	0.000	6	0.000	0.000	0.000	0.000

3
METCALC - EPRI METRIC CALCULATOR

EPRI MetCalc is a software tool that EPRI developed to support utilities that seek to use the cyber security metrics in their environment. It is a stand-alone graphical user interface (GUI)-based application that runs on the Microsoft Windows operating system, with functionality to:

- Load pilot data
- Calculate a base set of metrics
- 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

EPRI MetCalc has three perspectives: data perspective, metric perspective, and dashboard perspective.

Data Perspective

The data perspective incorporates functions to load and/or clean data. The left pane shows the names of 12 standard data tables (see Figure 3-1). When a user selects a data table name, the loaded data rows are displayed on the main pane.

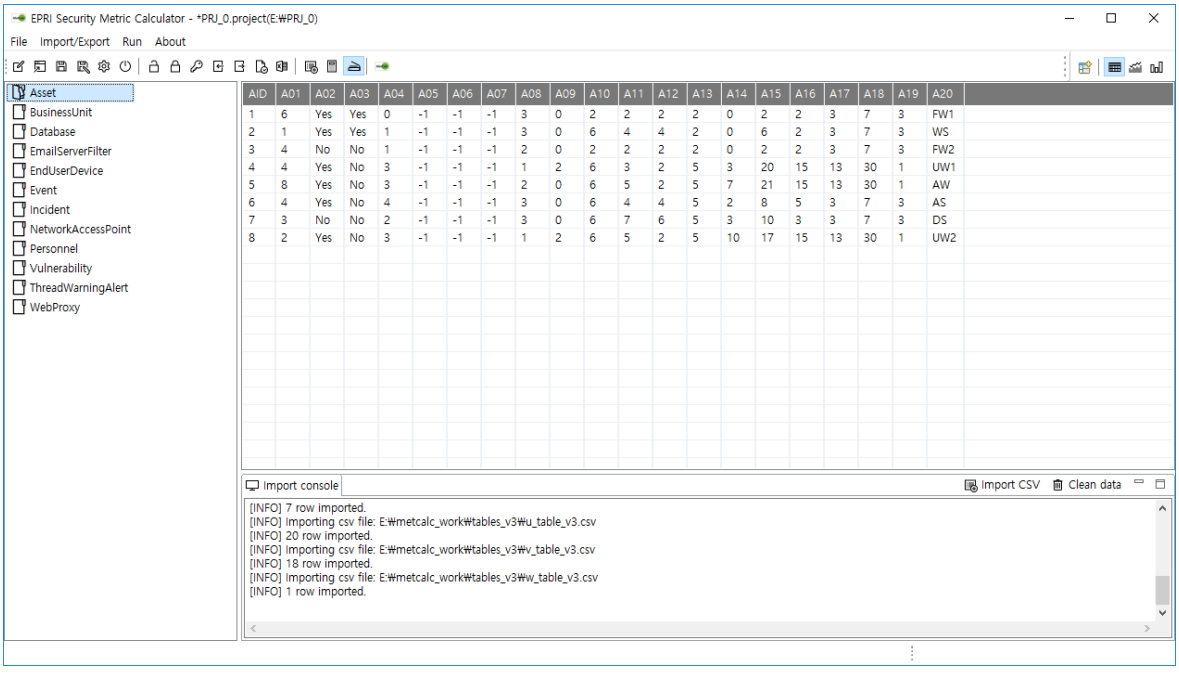

Figure 3-1
EPRI MetCalc – data perspective

Metric Perspective

The metric perspective incorporates functions to calculate metrics from the loaded data. The metrics are organized in the EPRI three-level tree structure of strategic, tactical, and operational metrics. For each metric, the following properties are displayed (see Figure 3-2):

- Metric ID
- Metric name
- Standard weight (editable)
- Metric value (calculated)
- Reference value (loaded from a .csv file)
- Target value (editable)
- Factors/factor values (editable)

Calculated metrics, weights, and factors can be exported into a Microsoft Excel file.

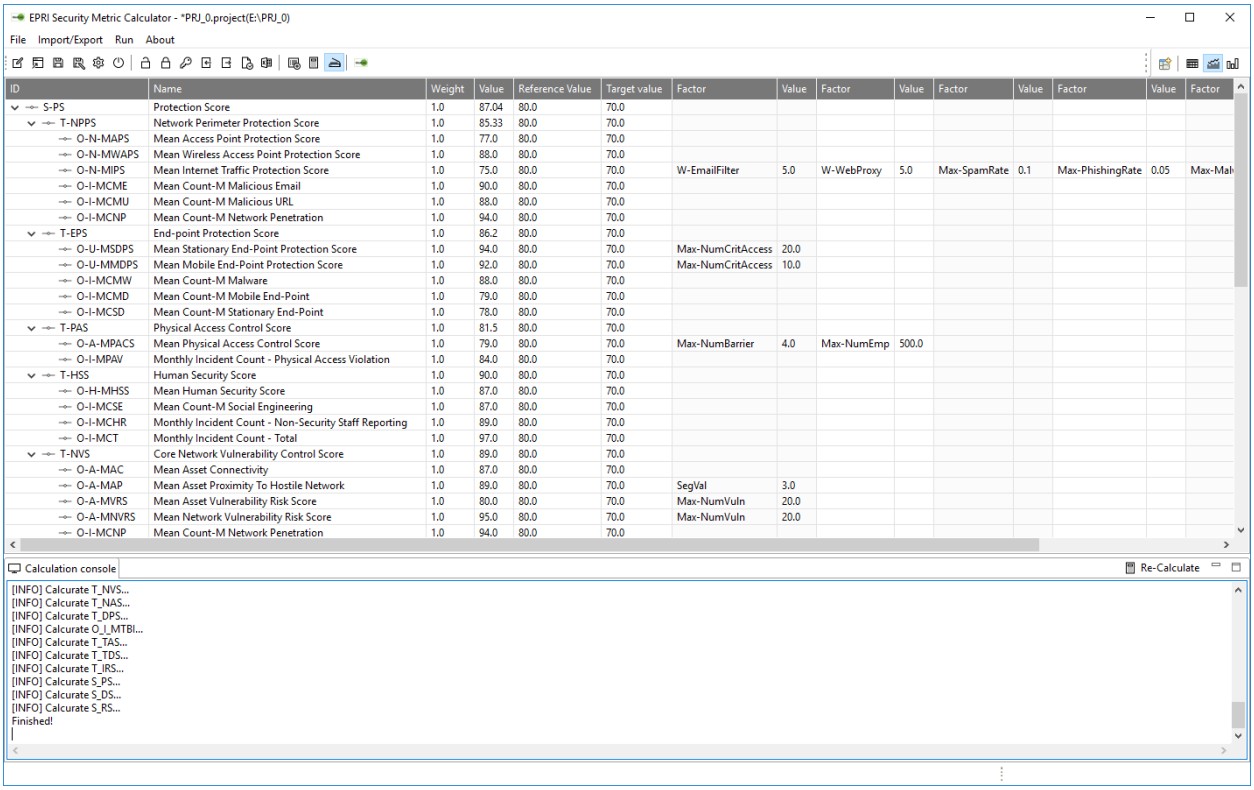

Figure 3-2
EPRI MetCalc – metric perspective

Dashboard Perspective

The dashboard perspective displays the calculated metrics visually. Each level of EPRI metric hierarchy employs a different display format. Strategic metrics are shown on the top left corner with three gauges. Historical trends of the strategic metric are displayed below the metric. Ten tactical metrics are displayed on the bottom left as a bar chart. Forth-seven operational metrics are displayed in tabular format on the right side of the display. To facilitate visual comparisons, the target value and reference value is shown for each metric (see Figure 3-3)..

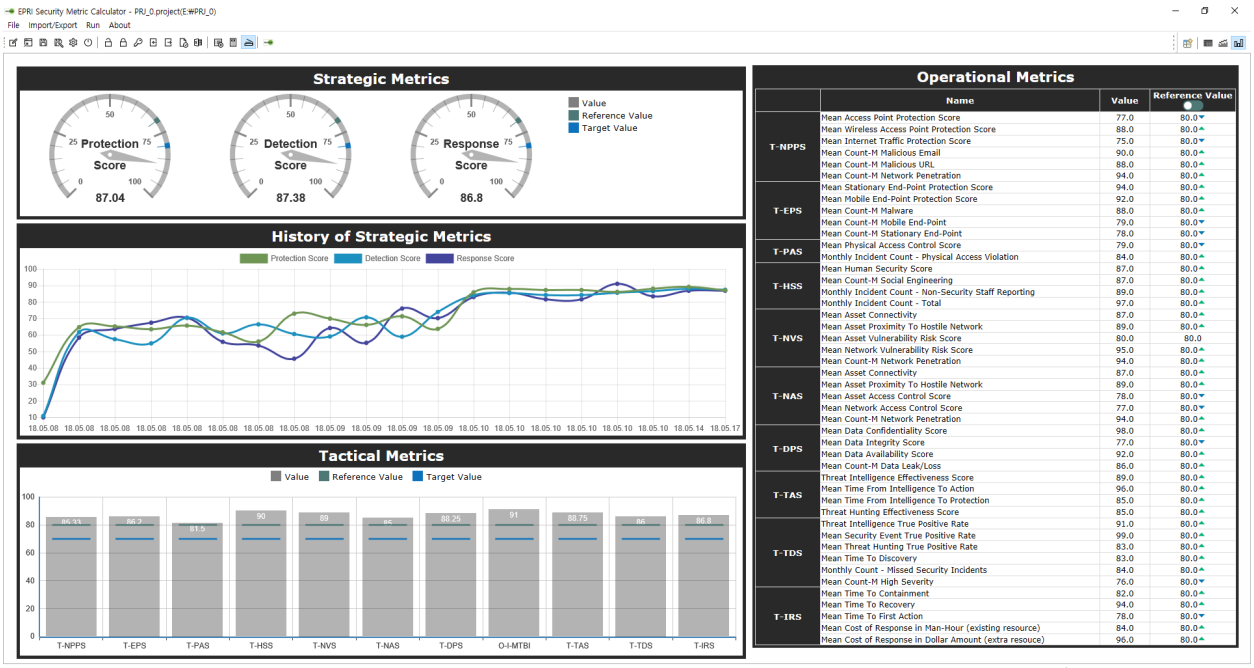

Figure 3-3
EPRI MetCalc – dashboard perspective

Currently, utilities pilot-testing EPRI cyber security metrics are beta-testing MetCalc. Once the study is complete, EPRI will release the software as an open-source application.

4
USABILITY SURVEY

An important next step for the EPRI cyber security metrics project is the operationalization of the metrics in day-to-day utility security operations. While EPRI is still enhancing the metric formulae and data points, utility members have actively discussed the usability of the EPRI metrics. In order to understand the needs of utility members and respond to the most pressing needs, the project conducted a usability survey during the 2018 Fall EPRI Advisory meeting. This section describes the results of the survey.

Survey Context

The survey was conducted in an informal setting using an online polling tool. The results were displayed in real-time on the projected screen, allowing instant review of the results and prompting discussions among the participants. EPRI posed a total of seven questions:

1. How difficult is it to understand EPRI metrics as a person being reported?
2. How difficult is it to explain EPRI metrics as a person reporting the score?
3. Would you be able to use EPRI metrics for your day-to-day operation?
4. Why or Why not?
5. What is the most critical barrier for EPRI metrics operationalization?
6. What is the one thing that will help you to operationalize EPRI Metrics?
7. If all three are available now, when would you start collecting data to use EPRI metrics?

The number of responses across the questions ranged from 13 to 21. Participants were provided the opportunity to answer anonymously or provide their names.

Survey Results

The tables and figures in this section summarize the answers for each question.

Q1: How Difficult Is It to Understand EPRI Metrics as a Person Being Reported?

This question measures the perception of difficulties in understanding the scores when they are presented to them. The result shows that EPRI metrics are considered to be relatively easy to understand when they are reported (see Table 4-1 and Figure 4-1).

Table 4-1
The degree of difficulty – reported

1 - very easy	2	3	4	5 - very difficult	Total
0	10	3	3	0	16
0%	63%	19%	19%	0%	100%

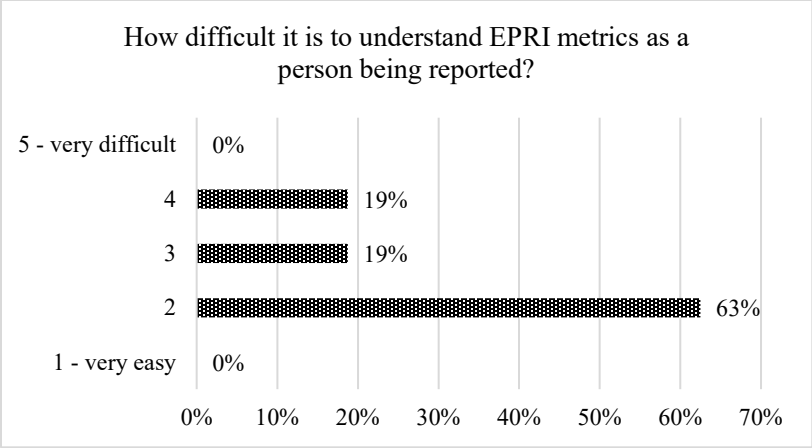

Figure 4-1
The degree of difficulty – reported

Q2: How Difficult Is It to Explain EPRI Metrics as a Person Reporting the Score?

This question measures the perceived difficulties of explaining EPRI metric scores to a stakeholder. The result shows that EPRI metrics are considered to be relatively difficult to explain (see Table 4-2 and Figure 4-2).

Table 4-2
The degree of difficulty – reporting

1 - very easy	2	3	4	5 - very difficult	Total
0	0	8	8	2	18
0%	0%	44%	44%	11%	100%

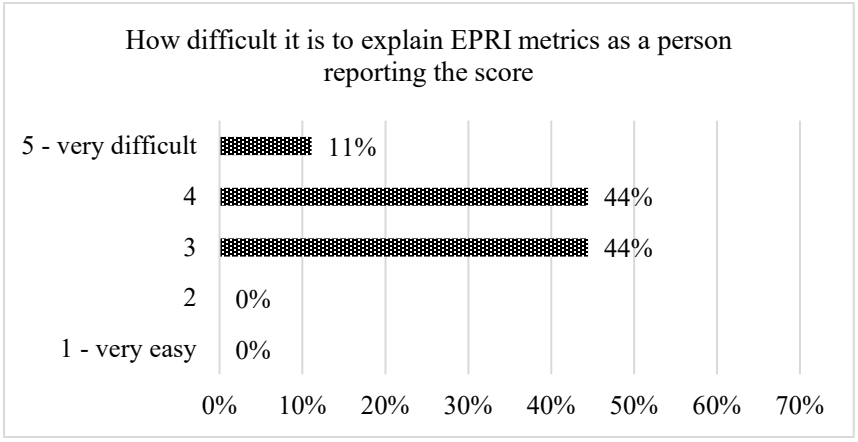

Figure 4-2
The degree of difficulty – reporting

Q3: Would you be able to use EPRI metrics for your day-to-day operation?

The question assesses the ease of utilizing EPRI metrics in their current state for day-to-day utility security operations. Exactly 50% of responders answered yes; and the other 50% responded no (see Table 4-3 and Figure 4-3). The reasons for their answers were requested in the next question, Q4.

Table 4-3
Day-to-day usability

Yes	No	Total
10	10	20
50%	50%	100%

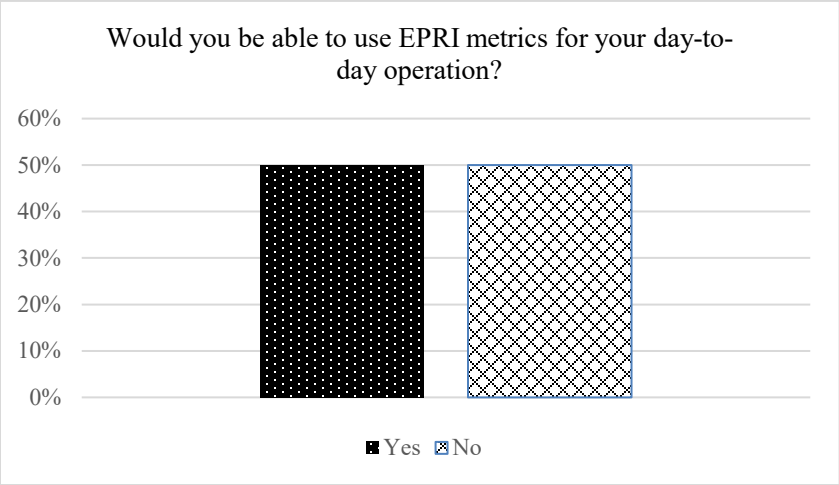

Figure 4-3
Day-to-day usability

Q4: Why or Why Not?

This question requests the reasons for answering yes or no in the previous question, Q3. Each respondent typed the reason in a free format. Although the question asks to specify the reasons for answering ”yes” or ”no,” a majority of respondents seemed to answer the question ”why not?,” assuming a ”no” response in the previous question. The result below is compiled by characterizing the free text format answers into five categories (see Table 4-4 and Figure 4-4):

- Difficulty in data collections
- Lack of knowledge or information
- Not the right level of details (too high-level, or too detailed)
- Tool not ready
- Other

Table 4-4
Reasons for day-to-day usability

Data collection difficulties	Not in the right level of details for my work	Lack of knowledge /information	Other	Tool not ready	Total
3	3	3	3	2	14
21%	21%	21%	21%	14%	100%

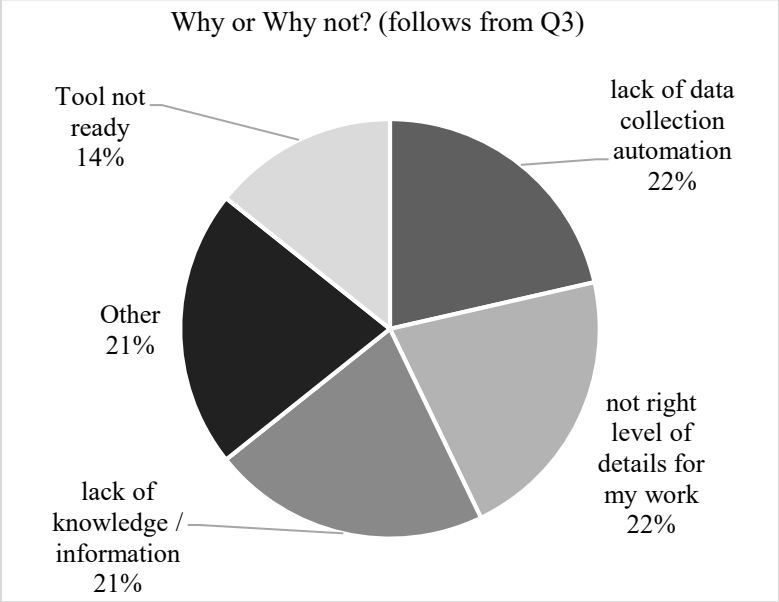

Figure 4-4
Reasons for day-to-day usability

Q5: What Is the Most Critical Barrier for EPRI Metric Operationalization?

This question measures the perceived barriers for operationalizing EPRI metrics in utility day-to-day operations. This question is closely related to Q4, in that it asks the same question, but provides four choices that the project team selected as the critical barriers. In response to this question, 52% selected ”complexity” as the primary barrier, and 38% selected ”other,” indicating the real pain point may not be listed in the choices given (see Table 4-5 and Figure 4-5).

Table 4-5
Barrier to operationalization

Complexity	Other	Inconsistency with the current program	Too many data points	Total
11	8	1	1	21
52%	38%	5%	5%	100%

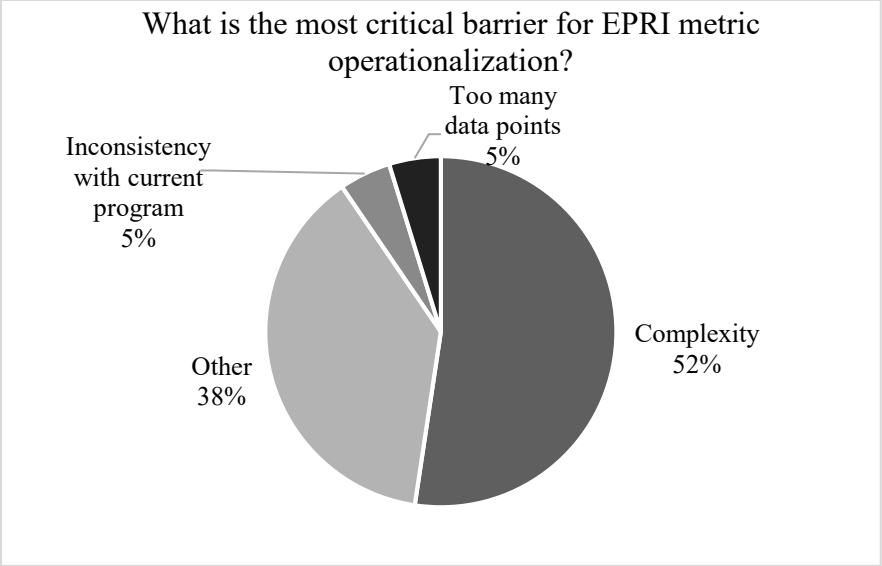

Figure 4-5
Barrier to operationalization

Q6: What Is the One Thing that Will Help You to Operationalize EPRI Metrics?

This question measures the perception of the possible catalysts for metric operationalization. Responders were given only three choices, without an option for comments. The results show some contrasts to the answers to Q5, where a majority indicated ”complexity” as the primary barrier. Rather than selecting simplification – a natural solution for the problem indicated – the majority indicated that more help in data collection, such as tools and guideline, would facilitate operationalization (see Table 4-6 and Figure 4-6).

Table 4-6
Catalysts for metric operationalization

Data collection tool/guideline	Simplification - reduce the number of metrics/data points	Mapping to CSF, C2M2, NERC-CIP, etc.	Total
13	4	0	17
76%	24%	0%	100%

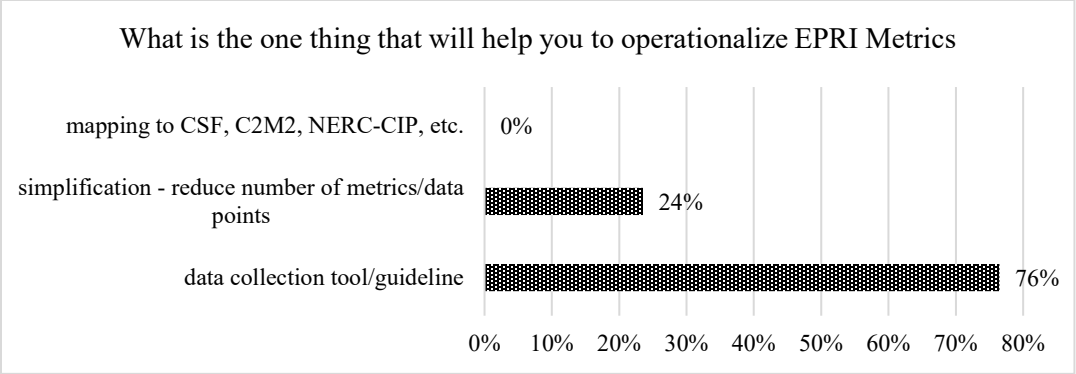

Figure 4-6
Catalysts for metric operationalization

Q7: If All Three (Tools) are Available Today, When Would You Start to Collect Data to Use EPRI Metrics?

This question measures the timing of intended EPRI metrics operationalization, given that necessary support and tools are available. Sixty-one percent answered "within one year," and 28% answered "right away." The result indicates that EPRI members are quite ready to operationalize metrics and expect EPRI to deliver the necessary tools and support (see Table 4-7 and Figure 4-7).

Table 4-7
Intended timing for metric operationalization

Within 1 year	Right away	Within 3 years	Not sure	Never	Total
11	5	1	1	0	18
61%	28%	6%	6%	0%	100%

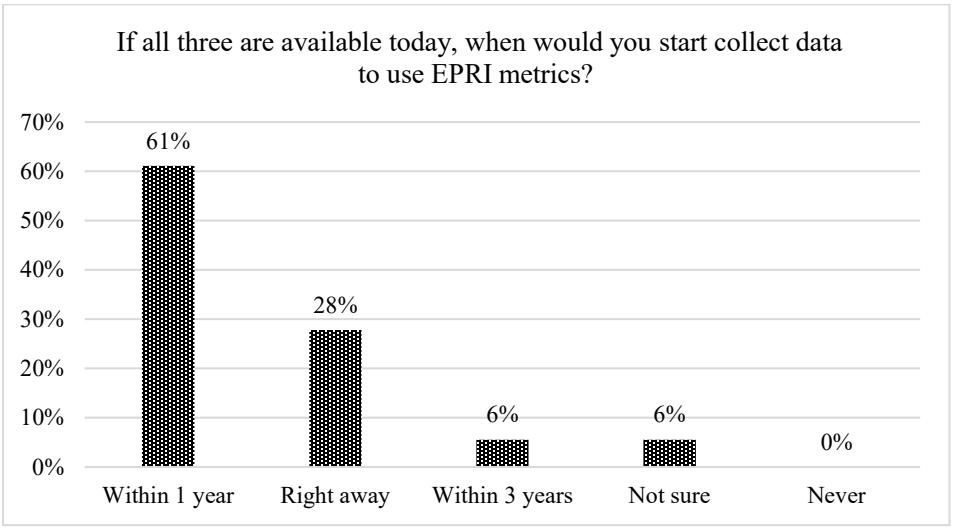

Figure 4-7
Intended timing for metric operationalization

5
NEXT STEPS

In the last three years, the EPRI cyber security metrics for the electric sector project has matured rapidly and garnered a high level of attention from EPRI members. Now, the project is poised to provide an end-to-end solution to enable the industry to measure the effectiveness of cyber security investments.

While EPRI is continuing work to improve the mathematics behind the metrics, the usability survey results identify important needed steps to facilitate broader adoption of the EPRI metrics. In response to these needs, the project will examine the following areas in future years:

- **Data Collection Guidelines and Tools.** The most pressing need identified in the usability survey is providing tools and guidelines for data collection to members interested in operationalizing metrics. EPRI will work with members to identify the data sources for the metric data, as well as to engage vendors in order to make tools that support data collection available in the market.
- **EPRI Metrics Light.** Project participants have suggested development of a simplified version of the EPRI metrics. The key to this research is to identify a way to simplify the metrics without losing the integrity of the mathematical foundation.
- **EPRI Metrics Hub**. With the support of EPRI's Technology Innovation program, the project team has conducted preliminary research on large-scale metric data aggregation. The research is ongoing, and preliminary results are expected to be available in early 2019.
- **Open MetCalc.** As discussed and planned, the MetCalc tool will be available to the public free of charge, once the pilot study is complete.
- **EPRI Metrics v.2.0.** EPRI Metrics Version 2.0 will feature improved formulae and data points utilizing lessons learned from the pilot-testing.
- **EPRI Metrics Advisory Council (MAC).** EPRI is establishing a public forum to continue enhancement of the metrics, tools, and aggregation with broader engagement of the industry.

Data-driven decision-making is an approach that values decisions that can be justified with verifiable data. This approach is an effective means of avoiding unconscious bias and of grounding decisions based on actual data. In the current landscape of cyber security for the electric sector, where there are many uncertainties and the stakes are high, data-driven decision-making is acutely needed. EPRI's cyber security metrics for the electric sector project aspires to provide an essential tool for data-driven cyber security in future years.

6
REFERENCES

1. *Creating Security Metrics for the Electric Sector*. EPRI, Palo Alto, CA: 2015. 3002005947. https://www.epri.com/#/pages/product/000000003002005947/.
2. *Creating Security Metrics for the Electric Sector, Version 2.0*. EPRI, Palo Alto, CA: 2016. 3002007886. https://www.epri.com/#/pages/product/000000003002007886/.
3. *Creating Security Metrics for the Electric Sector, Version 3*.0. EPRI, Palo Alto, CA: 2017. 3002010426. https://www.epri.com/#/pages/product/000000003002010426/.
4. National Institute of Standards and Technology (NIST), U.S. Department of Commerce, "Framework for Improving Critical Infrastructure Cybersecurity," draft update, January 10, 2017, https://www.nist.gov/news-events/news/2017/01/nist-releases-update-cybersecurity-framework.
5. North American Electric Reliability Corporation (NERC), "Critical Infrastructure Protection (CIP) Standards," website, http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx.
6. National Institute of Standards and Technology (NIST), U.S. Department of Commerce, "Performance Measurement Guide for Information Security," NIST SP 800-55, revision 1, July 2008, http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-55r1.pdf.
7. National Institute of Standards and Technology (NIST), U.S. Department of Commerce, "Guidelines for Smart Grid Cybersecurity," The Smart Grid Interoperability Panel – Smart Grid Cybersecurity Committee, NISTIR 7628 Revision 1, September 2014, http://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.7628r1.pdf.
8. U.S. Department of Energy, "Cybersecurity Capability Maturity Model (C2M2)," website, https://energy.gov/oe/cybersecurity-critical-energy-infrastructure/cybersecurity-capability-maturity-model-c2m2-program

Export Control Restrictions

Access to and use of this EPRI product is granted with the specific understanding and requirement that responsibility for ensuring full compliance with all applicable U.S. and foreign export laws and regulations is being undertaken by you and your company. This includes an obligation to ensure that any individual receiving access hereunder who is not a U.S. citizen or U.S. permanent resident is permitted access under applicable U.S. and foreign export laws and regulations.

In the event you are uncertain whether you or your company may lawfully obtain access to this EPRI product, you acknowledge that it is your obligation to consult with your company's legal counsel to determine whether this access is lawful. Although EPRI may make available on a case by case basis an informal assessment of the applicable U.S. export classification for specific EPRI products, you and your company acknowledge that this assessment is solely for informational purposes and not for reliance purposes.

Your obligations regarding U.S. export control requirements apply during and after you and your company's engagement with EPRI. To be clear, the obligations continue after your retirement or other departure from your company, and include any knowledge retained after gaining access to EPRI products.

You and your company understand and acknowledge your obligations to make a prompt report to EPRI and the appropriate authorities regarding any access to or use of this EPRI product hereunder that may be in violation of applicable U.S. or foreign export laws or regulations.

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 members represent 90% of the electric utility revenue in the United States with international participation in 35 countries. EPRI's principal offices and laboratories are located in Palo Alto, Calif.; Charlotte, N.C.; Knoxville, Tenn.; and Lenox, Mass.

Together…Shaping the Future of Electricity

3002013690

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