EPRI | ELECTRIC POWER RESEARCH INSTITUTE

Creating Security Metrics for the Electric Sector, Version 2.0

3002007886

Creating Security Metrics for the Electric Sector, Version 2.0

3002007886

Technical Update, December 2016

EPRI Project Manager

A. 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 Investigators
C. Suh-Lee
A. Lee

This report describes research sponsored by EPRI.

(Jason Christopher authored the 2015 version of this report.)

EPRI would like to acknowledge the support of the following organizations:

- Edison Electric Institute
- American Public Power Association
- National Rural Electric Cooperative Association
- Utilities Technology Council
- SANS Institute
- North American Transmission Forum

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

Creating Security Metrics for the Electric Sector, Version 2.0. EPRI, Palo Alto, CA: 2016. 3002007886.

ABSTRACT

The nation's power system is a complex machine consisting of both legacy and next generation technologies. Daily reliable operation of the power grid relies on intelligent components that communicate with advanced capabilities. Cyber security focuses on the ability to protect these unique systems and devices from being disrupted, disabled, destroyed, or maliciously controlled. This includes the destruction and theft of data or the compromise of data availability and integrity. While the electricity sector has matured in the protection of critical systems and devices, many security practitioners struggle with quantifying cyber security program improvements.

To better protect the nation's power grid, many utilities are investigating methods of communicating their security posture across the organization as well as to outside parties. This has led to several discussions regarding measuring cyber security in a consistent manner. Building on previous efforts, the electricity industry leverages various security metrics and is constantly maturing in this relatively new field.

This technical update provides guidance to utilities on developing and implementing a security metrics program leveraging existing best practices. The guidance is intended to complement existing cyber security and compliance programs.

Keywords
Cyber security
Cyber security risk management
Cyber security metrics
Information assurance

Deliverable Number: 3002007886

Product Type: Technical Update

Creating Security Metrics for the Electric Sector, Version 2.0

PRIMARY AUDIENCE: Power delivery system owners and operators

SECONDARY AUDIENCE: Research organizations and solution providers

KEY RESEARCH QUESTION

Cyber security programs in utility environments lack robust and meaningful metrics to link performance and efficiency to security risk management. Security metrics need to be explored and implemented to ensure that appropriate improvements are made to decrease cyber security risk.

RESEARCH OVERVIEW

Utilities have unique considerations for creating or updating a security metrics program. These could include specific concerns with regulations, enhancing existing capabilities, or simply trying to manage security risk by measuring program goals and efficiencies. Moreover, utilities must manage their security programs across both traditional information technology (IT) systems as well as highly specialized operations technology (OT) systems, including industrial control systems. These OT systems, which lack modern security capabilities, will not benefit from automated sources of data collection—a key step towards implementing security metrics. The core elements of this research outline the uses for metrics and leverage existing guidance for a basic metrics program. In 2015, EPRI collaborated with members and external partners to create and vet a template for creating security metrics. In 2016, EPRI developed a set of potential metrics and data points that may be used in a security metrics program.

KEY FINDINGS

- This guidance is intended to address the creation and implementation of a cyber security metrics program within any utility, regardless of size, function, or ownership structure. The concepts introduced in this document can apply to both IT and OT and their associated cyber security practices. The guidance is not intended to replace current cyber security activities, programs, processes, or approaches. Rather, it is meant to complement existing efforts in a comprehensive enterprise cyber security risk management program.
- Data will need to be collected across internal organizational boundaries and reported at various levels, with results directed to managers and executives. Senior managers and executives must be engaged prior to establishment of security metrics.
- Many existing efforts can complement a security metrics program, including mandatory regulations and voluntary adoption of security frameworks.
- Security metrics can supplement data needed for security architectures, integrated security operation centers (ISOCs), and common operating pictures (COPs).

WHY THIS MATTERS

This research explains the steps needed to create a security metrics program and provides a suite of potential metrics that can relate the allocation of staff, processes, and tools to enterprise risk management. Once implemented, a security metrics program may be communicated in a manner similar to how reliability and safety indices are reported throughout business units and to senior management.

HOW TO APPLY RESULTS

Any utility developing a security metrics program should engage with senior management and executives first. As a relatively new field, security metrics is not as mature or robust as metrics in finance, reliability operations, or safety. Therefore, security practitioners will need to set realistic expectations and establish direct links to the enterprise risk management program. From there, the guidance in this document can be applied, with tailoring of the metrics template and selection of the various metrics and data points.

The North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Standards are referenced throughout this document as an example of using existing programs when implementing a cyber security metrics program. This guidance document does not provide further information on achieving compliance with NERC CIP, as the focus is on the larger security program that may exist across the enterprise and not just for the bulk electric system. The NERC CIP compliance authority should be consulted for any questions on NERC CIP compliance.

LEARNING AND ENGAGEMENT OPPORTUNITIES

- Collaborators: Edison Electric Institute (EEI), National Rural Electric Cooperative Association (NRECA), American Public Power Association (APPA), and Utilities Technology Council (UTC)
- Presentation materials: EPRI 2016 Cyber Security Technology Transfer Workshop, held November 1–2, 2016, in Dallas, TX
- EPRI 2017 Winter Advisory Meeting, held February 13–15, 2017, in Huntington Beach, CA

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

PROGRAM: Cyber Security, 183

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

CONTENTS

LIST OF FIGURES

LIST OF TABLES

1
INTRODUCTION

Background and Purpose

Over the past decade, the electric sector has produced both mandatory and voluntary standards and guidelines to address cyber security. Each of these attempts to enhance the security posture of a utility, despite the fact that each utility has unique environments, ownership structures, and functions for the overall reliability of the nation's power grid. These standards and guidelines were developed in similar ways to the sector's creation of documents in other fields—balancing of load and generation, management of reliability events, and other functions required for reliable operations. The science and engineering behind power systems dates back to the late 1800s, with thousands of studies and measurement behind each model used for planning and operations. Unfortunately, cyber security is not as mature—as a field, the science involved in protecting digital systems has only existed for a fraction of the history shared with power systems engineering. Over the past two decades, research has continued to evolve in the field of cyber security measurement. These advancements make it possible to implement a cyber security metrics program within any utility, regardless of size, organization, or ownership structure.

There are several challenges with cyber security metrics. While there are many business and regulatory pressures driving utilities to improve process efficiency, there is also a lack of data sharing required to have a dialogue regarding "what metrics matter" in cyber security. As a result, security metrics routinely focus on standards development or other frameworks that may not be entirely appropriate for measurement.

The purpose of this document is to provide a methodology for creating a security metrics program that complements existing cyber security activities. This research effort will include a standardization of terms and definitions, as well as the use of a metrics template and base set of security metrics. Due to an organization's unique security posture, the creation of a metrics program will need to be tailored. In the following sections, this document highlights the actions needed to create, tailor, and manage a security metrics program, as well as a sample template for security metrics (Appendix A).

Definitions and Concepts

All measurements, whether in science, engineering, or mathematics, have varying degrees of usefulness. Since metrics and measurements come in varying types, the first step in establishing a security metrics program is to decide what metrics matter. This document will explore metrics and how to establish a security metrics program in a utility's various information technology (IT) and operations technology (OT) environments. In order to do so, some key definitions and

concepts need to be established. Section 5 contains a glossary of other terms and acronyms used in this document. The definitions for *measure* and *metric* are extracted from a NIST article[1].

- A **measure** is a concrete, objective attribute, such as the percentage of systems within an organization that are fully patched, the length of time between the release of a patch and its installation on a system, or the level of access to a system that a vulnerability in the system could provide.
- A **metric** is an abstract, somewhat subjective attribute, such as how well an organization's systems are secured against external threats or the effectiveness of an organization's incident response team. An analyst can approximate the value of a metric by collecting and analyzing groups of measures.
- **Measurement:** The process to determine a value [ISO 27004]

In this document, measures will typically be used in the computation of metrics. Utilities can, and should, measure things at different levels of the organization, as illustrated below in Figure 1-1.

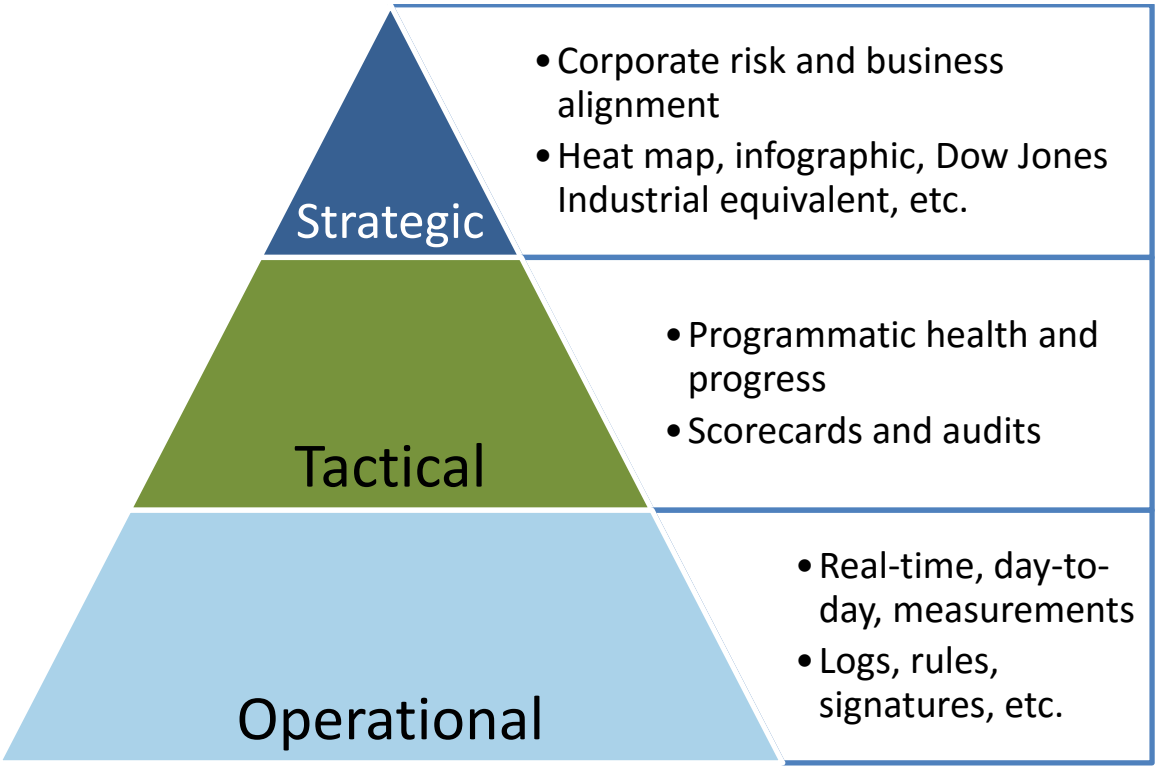

Figure 1-1
Organizational levels and various metrics and measures

[1] CYBER SECURITY METRICS AND MEASURES Paul E. Black, Karen Scarfone and Murugiah Souppaya National Institute of Standards and Technology, Gaithersburg, Maryland, included in *Wiley Handbook of Science* and Technology for Homeland Security, Edited by John G. Voeller Copyright © 2008 John Wiley & Sons, Inc.

Each level of the organization, ranging from operational to strategic, will have useful data for measuring cyber security. Since each utility has different governance structures, Figure 1-1 is not intended to prescribe organizational roles or communication. Rather, the diagram outlines that at each level of an organization there is a different audience and available data.

- **Operational Levels** is where much of the raw data used for metrics will be collected. This is where security practitioners address events and incidents, review logs, and manage security systems. The data analyzed at this level can be used to help evaluate efficiencies and implementations of new controls.
- **Tactical Levels** include most program management objectives. The metrics computed here should answer the question, "How well is the security program doing?" Most third-party evaluation techniques already examine program management; however, rarely do those evaluations tie back to the operational data.
- **Strategic Levels** are typically where business executives and boards, or equivalent, reside. While costs and efficiencies are important, in today's security environment, most executives want to know, "How secure are we?" This is not the same audience as for the tactical metrics. Moreover, most security managers are challenged to summarize large volumes of technical data into displays or relate program activities back to corporate risk.

A successful security metrics program will pull together measurement activities, data, and reports for each of these organizational levels. More importantly, a mature security metrics program will communicate the relationships between operational data, tactical program activities, and strategic risk management governance. This document will specify some of the techniques that can be used to establish metrics program activities, with specific consideration for a utility's unique environment.

2
USING SECURITY METRICS

Today, most utilities understand the complicated nature of cyber security risk. Unfortunately, when discussing this risk across an organization, many security practitioners across industry default to a qualified discussion of "high, medium, and low" threats, vulnerabilities, and impacts. The purpose of a security metrics program is to mature the dialogue that takes place among security practitioners, managers, and business leaders. A security metrics program requires a certain level of maturity within an organization and other factors to succeed, including management support and adequate resources to support data collection and analysis. Any associated costs with creating a security metrics program may be offset by a greater understanding of a utility's threat profile and security posture across multiple business units and facilities. A cyber security metrics program can assist a utility by:

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

To achieve these goals, a security metrics program will need to be informed by existing metrics efforts, including those in other parts of the organization, such as finance or human resources. These metric programs will also need to be incorporated into an existing enterprise risk management approach. By creating interdependencies between metrics, management decisions, and risk, a utility creating a cyber security metrics program can ensure common terminology and concepts across leadership and practitioners, while also leveraging lessons learned from different, and possibly more mature, efforts. Figure 2-1 below illustrates the various components of a cyber security program and the role of security metrics. The acronyms are:

- C2M2: Cybersecurity Capability Maturity Model
- NERC CIP: North American Electric Reliability Corporation Critical Infrastructure Protection
- NIST: National Institute of Standards and Technology
- NISTIR: NIST Interagency Report
- SP: Special Publication

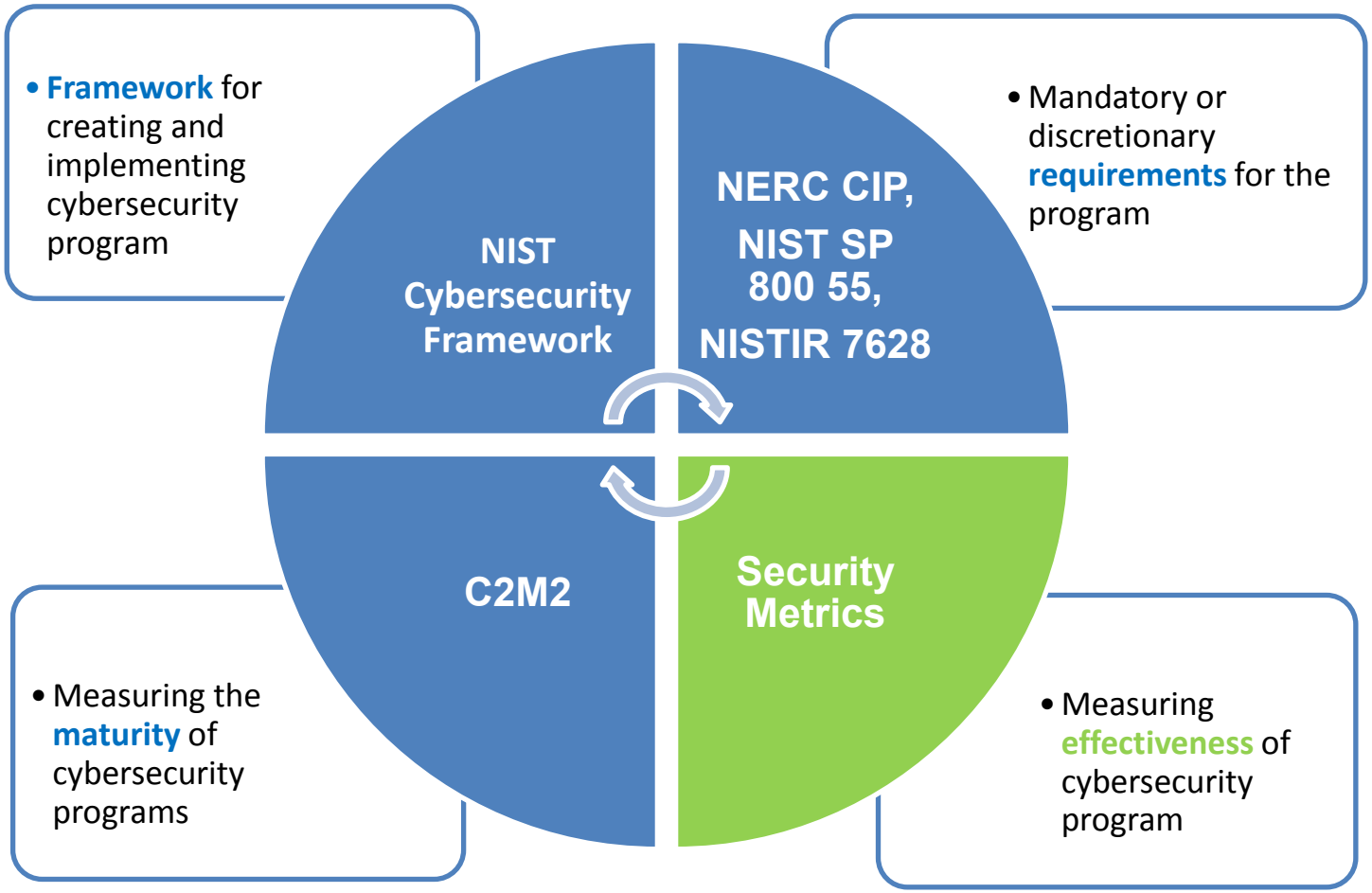

Figure 2-1
Security Metrics Program within an Organization

This section examines the qualities of robust metrics and their application to cyber security. Since most, if not all, security programs rely heavily on standards, new metrics will need to complement existing security controls and management decisions. The concepts highlighted below can aid utilities in identifying useful principles for creating a metrics program, as outlined in Section 3.

Security Standards and Guidelines as Inputs for Metrics

Cyber security as a field is typically defined by security standards and guidelines. These standards and guidelines provide requirements for both regulated and voluntary security programs to implement and are usually based on risk associated with assets or systems. In traditional IT environments, there have been several notable standards/guidelines used across industry, including the International Organization for Standardization (ISO) 2700X series and National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53. Within the electric sector, industry has created sector-specific requirements in both the mandatory North American Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Reliability Standards, as well as voluntary controls in the NIST Interagency Report (NISTIR) 7628 *Guidelines for Smart Grid Cybersecurity*. These standards/guidelines, and others, make up the foundation for many security programs as they provide an industry-agreed upon norm for utilities to implement core security practices.

Security standards/guidelines are not the same as security metrics. Security metrics should facilitate analysis and discussion, while providing insight into program improvements or gaps. Standards/guidelines provide a common taxonomy for discussing cyber security threats and vulnerabilities. Some standards detract the focus from process improvement towards compliance.

To implement a security metrics program, organizations need to understand that compliance and security are efforts that should complement each other. Security standards, such as NERC CIP, are core components to any program. Security metrics can enable measurement and improvement of security standard requirements as they pertain to overall risk beyond compliance. Standards, especially mandatory ones such as NERC CIP, may only provide one data set needed for overall security metrics. Standards alone will not be adequate for a metrics program. In particular, a solely CIP-based metrics program would suffer from the following:

- **Focused on compliance:** The NERC CIP standards focus on mandatory compliance. The standards provide guidance on what assets need to be selected with various requirements implemented across the organization. There is no guidance or recommendations on how to manage, monitor, or measure the effectiveness of those controls. If a metrics program were based on NERC CIP, the highest form of achievement would be to comply with the standards, not continuous improvement.
- **Not focused on metrics:** Many of the other technical NERC standards have metrics. For example, NERC Reliability Standard BAL-002 requires the computation of a recovery ratio through a disturbance. The compliance "metric" includes the ratio. NERC CIP only requires documentation that a requirement has been implemented. NERC CIP is designed to provide baseline protections for North America federal regulatory purposes—it was not designed to measure effectiveness or management of security controls.

While this document includes language to complement the electric sector's work in standards, there will not be any CIP-derived or other standards-derived metrics in this guidance document. Instead, such standards will be referenced where applicable.

Leveraging Maturity Models and Roadmaps

For the reasons outlined above, security standards alone are not adequate for establishing a cyber security metrics program. Many utilities may use efforts similar to those outlined in the NIST Cyber Security Framework (CSF) or maturity models such as the Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2)[2]. These efforts are a good starting point for any utility branching into security metrics. These efforts allow an organization to quickly assess their current capabilities and outline plans for future states. Many of these activities go *beyond* what is found in baseline compliance standards and can help an organization prioritize security investments.

While prioritization and assessing capabilities may provide a starting point, there are many reasons why the CSF or alone cannot represent a security metrics program. First, and perhaps most important, neither can measure efficiency (such as frequency or automation) of a practice. The capabilities are assessed in terms of "crawl, walk, run" and not in terms of running at a certain "speed." Second, each model or assessment needs to be tailored to a utility's individual risk profile, which already implies a certain level of maturity to do so. Moreover, many of the practices outlined in the CSF and C2M2 *require* security metrics to already be implemented. For example, the C2M2 Situational Awareness (SA) domain has a set of practices related to the Common Operating Picture (COP) that discusses the "state of cybersecurity" within an organization. Presumably, this requires a utility to already have an idea of steady state versus emergencies or ongoing incidents facing the IT and OT networks. To report on that state, utilities must have some way of measuring their current operations maintained by a set of metrics.

There are many ways that maturity models and roadmaps can be used to support a security metrics program. This will be discussed more in the next section.

Principles for Using Metrics

Metrics are used in many different fields and can be applied to various areas of an organization. While the field of security metrics is relatively new when compared to a utility's traditional power systems engineering measures, there are many existing metric qualities that can be applied to cyber security. As discussed, standards-based compliance programs may have *input* into a set of useful security metrics, but any new security metrics will need to be tailored to organizational goals and enterprise risk management practices.

These new metrics should follow the principles outlined from existing research, as noted below. There are several authoritative documents and concepts on metric development. The excerpts and cited works in this section should provide a base level of understanding on qualities, goals, and principles surrounding the use of security metrics in the utility environment. Additional resources can be found in Section 5.

---

[2] For the balance of this report, the more generic C2M2 will be referenced.

S.M.A.R.T.

For over 30 years, program management professionals have been using the S.M.A.R.T criteria for creating business objectives [1]. There are various versions of the acronym, though the objectives are largely the same. For the purposes of this guidance document, S.M.A.R.T. will refer to:

- **S**pecific: The security metric should not be ambiguous, but instead provide specific areas for improvement and targets or trends.
- **M**easurable: Each metric should identify indicators for success, using available data.
- **A**ctionable: The security metrics must be easy to understand and incorporated into program improvements.
- **R**elevant: Each security metric must tie back to program or risk priorities in a meaningful way.
- **T**ime-related: Measurement activities for security metrics must be based on timely access to (and reporting of) data.

Applying these objectives to any metric is a strong starting point to evaluating what measurement activities should take place within a security program.

Practical Measurement Framework for Software Assurance and Information Security

In 2008, the Department of Defense (DoD), Department of Homeland Security (DHS), and NIST Software Assurance Measurement Working Group released Version 1.0 of the *Practical Measurement Framework for Software Assurance and Information Security.* While not tailored explicitly for utilities or OT systems, the document outlines actionable guidance for any organization interested in security metrics. Specifically, utilities should consider the following principles when implementing a measurement approach, as found in the framework: [2]

- Cyber security measurement is a composite discipline which, to be most effective, should be integrated into an organization's existing measurement and risk management practices.
- Cyber security measures development and implementation initiatives can be incorporated into whatever measurement methodology is already being used.
- Cyber security measurement must satisfy information needs for a variety of stakeholders/audiences, including executives, developers, vendors, suppliers and acquirers.
- Each stakeholder group will require tailoring of specific measures based on each group's information needs.
- Different measures targeting different stakeholders may use the same information originating from the same data sources to facilitate multiple uses of the same set of data.
- Cyber security measures must be effective, practical, and worth the investment of resources in the long term.
- Implementation of cyber security measurement should incorporate automation to assist analysts in data collection, analysis, and reporting.

The working group's 2008 report contains a more complete look at software assurance measurement. [2]

Performance Management Guide for Information Security

Also in 2008, NIST released SP 800-55 "Performance Management Guide for Information Security." This guidance document outlines several components for implementing security metrics in federal agencies that must comply with NIST SP 800-53 controls. NIST SP 800-55, while focused on Federal Information Security Management Act (FISMA) compliance, offers benefits for the electric sector in implementing security metrics:

- **Increase Accountability:** Cyber security measures can increase accountability for information security by helping to identify specific controls that are implemented incorrectly, are not implemented, or are ineffective. Data collection and analysis processes can facilitate identification of the personnel responsible for security controls implementation within specific organizational components or for specific information systems. [3]
- **Improve Information Security Effectiveness:** A cyber security measurement program will enable organizations to quantify improvements in securing information systems and demonstrate quantifiable progress in accomplishing strategic goals and objectives. [3]
- **Demonstrate Compliance:** Organizations can demonstrate compliance with applicable laws, rules, and regulations by implementing and maintaining an information security measurement program. [3]
- **Provide Quantifiable Inputs for Resource Allocation Decisions:** Use of information security measures will support risk-based decision making by contributing quantifiable information to the risk management process. It will allow organizations to measure successes and failures of past and current information security investments, and should provide quantifiable data that will support resource allocation for future investments. Using the results of the analysis, program managers and system owners can isolate problems, use collected data to justify investment requests, and then target investments specifically to the areas in need of improvement. By using measures to target security investments, these measures can aid organizations in obtaining the best value from available resources. [3]

Metric Template

To aid utilities in the electric sector with creating and using security metrics, this document has leveraged the template from NIST SP 800-55 and tailored it to address utility-specific environments. Beyond the use of NIST security controls, the new sector-specific template incorporates NIST CSF and C2M2 references, and allows for consideration of compliance objectives for the NERC CIP Standards. The template notes the differences that may be associated with collecting data in OT environments, which differ from traditional IT systems and devices. More details on the template can be found in Appendix A.

The next section takes the concepts discussed in this section and applies them to the creation of a security metrics program in a utility's operational environment.

3
CREATING A CYBER SECURITY METRICS PROGRAM

Evaluating Security Program Goals and Capabilities

Prior to capturing security metrics, a utility will need to evaluate its basic security capabilities and program goals. While there may be value in measuring aspects of security gaps in a relatively less sophisticated security program, there will be far greater benefits to allocating resources towards implementation of security controls than to a security metrics program.

Thus, a good starting point would be to implement the C2M2. The C2M2, as a maturity model, helps utilities evaluate their cyber security capabilities across industry-defined goals for both sophistication of specific program elements and management objectives. As a one-day self-evaluation, the C2M2 provides a relatively easy entry into the world of security metrics. The C2M2 results can provide direct input into the tactical level discussion points from Figure 1-1 and may be leveraged to prioritize the detailed operational level metrics that should be created.

After performing a C2M2 self-evaluation, utilities should analyze their results and prioritize improvements. If there are any elements of a domain that are a maturity indicator level (MIL) of 0, then those should be addressed *prior* to developing a security metrics program. An ideal candidate for a robust security metrics program should be a utility that is *at least* a MIL 1 across all 10 domains, with a few domains at a MIL 2 or 3, depending on the organization's risk profile.

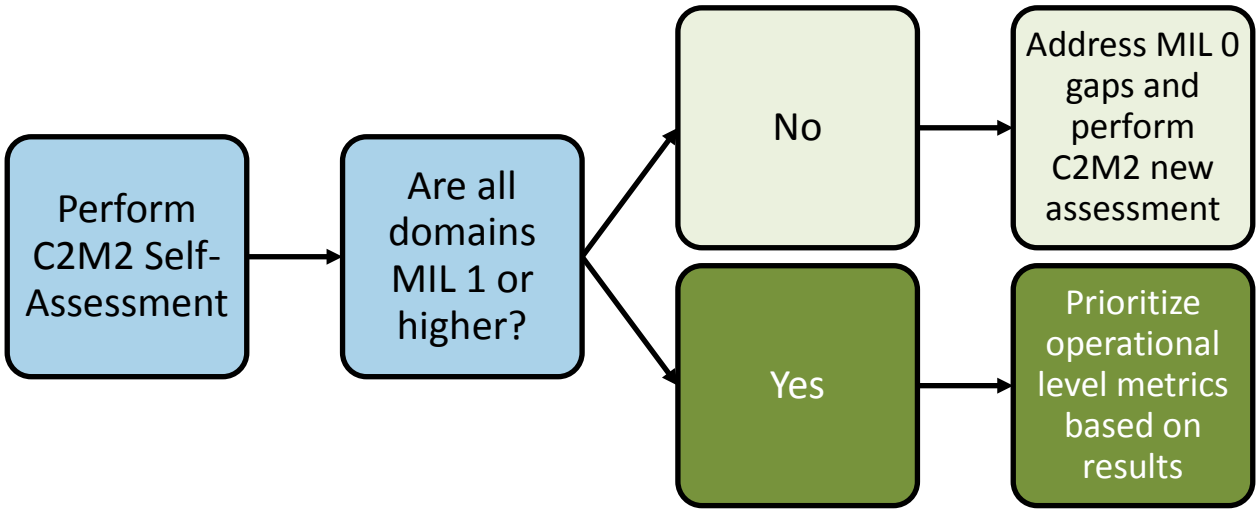

Figure 3-1
Leveraging C2M2 to evaluate readiness for security metrics program

As Figure 3-1 illustrates, any utility that is not at least at a MIL 1 across all C2M2 domains should address those gaps and then perform a new self-evaluation. Utilities that are at MIL 1 or greater should use the C2M2 to prioritize the operational metrics that should be evaluated to support their answers. For example,

- Were there any C2M2 practices that were fully or largely implemented that could be improved with metrics? Can data supporting those practices be collected through automated means?
- For practices that may be ad hoc in MIL 1, can metrics be used to promote documentation and policies?
- If a stated goal is to implement a Common Operating Picture (COP) from the C2M2 Situational Awareness (SA) domain, what metrics should be used to inform the creation of a COP?

These C2M2 considerations, combined with other organizational goals, can be implemented into an existing cyber security metrics program or the creation of a new program, as outlined below.

Existing Metrics and Risk Management Efforts

In many cases, utilities already have metrics programs. Typically, these programs are operationally focused, such as the programs leveraging reliability indices. It is important for any new metrics program to leverage current practices and lessons learned from existing programs. Ideally, the security metrics program would be included in existing operational measurement programs. When considering how to implement a security metrics program from existing resources or programs, the following questions may be useful:

- How are metrics currently tied into risk management discussions at the strategic level in Figure 1-1?
- Where is the data for measurement located? Who owns it? Who can collect it? The template in Appendix A highlights other basic considerations for metrics.
- What resources are allocated to metric collection and reporting?
- What subject matter expertise needs to be provided through an existing program to make the data meaningful?

If a metrics program already exists, security teams can inherit benefits from existing organizational objectives and governance.

Implementing a Security Metrics Program

In the cases where an existing measurement program cannot be leveraged, or where ownership of security metrics will reside with the existing security team, practitioners will need to outline a basic procedure for metric development and implementation. The aforementioned *Practical Measurement Framework for Software Assurance and Information Security* highlights a common framework for cyber security metrics that may be applied to a utility [2]:

- Creating cyber security metrics or updating existing metrics to include cyber security;
- Collecting data to support cyber security metrics;

- Storing collected data in a metrics repository;
- Analyzing collected data and compiling it into cyber security metrics;
- Normalizing and triangulating the metrics to determine causes of observed cyber security performance;
- Documenting and reporting cyber security metrics to appropriate stakeholders;
- Using metrics to support decision making and resource allocation; and
- Training measurement staff coupled with continuous improvement of metrics to ensure metrics are relevant to the project or organization.

This framework, including continuous improvement is illustrated in the figure below.

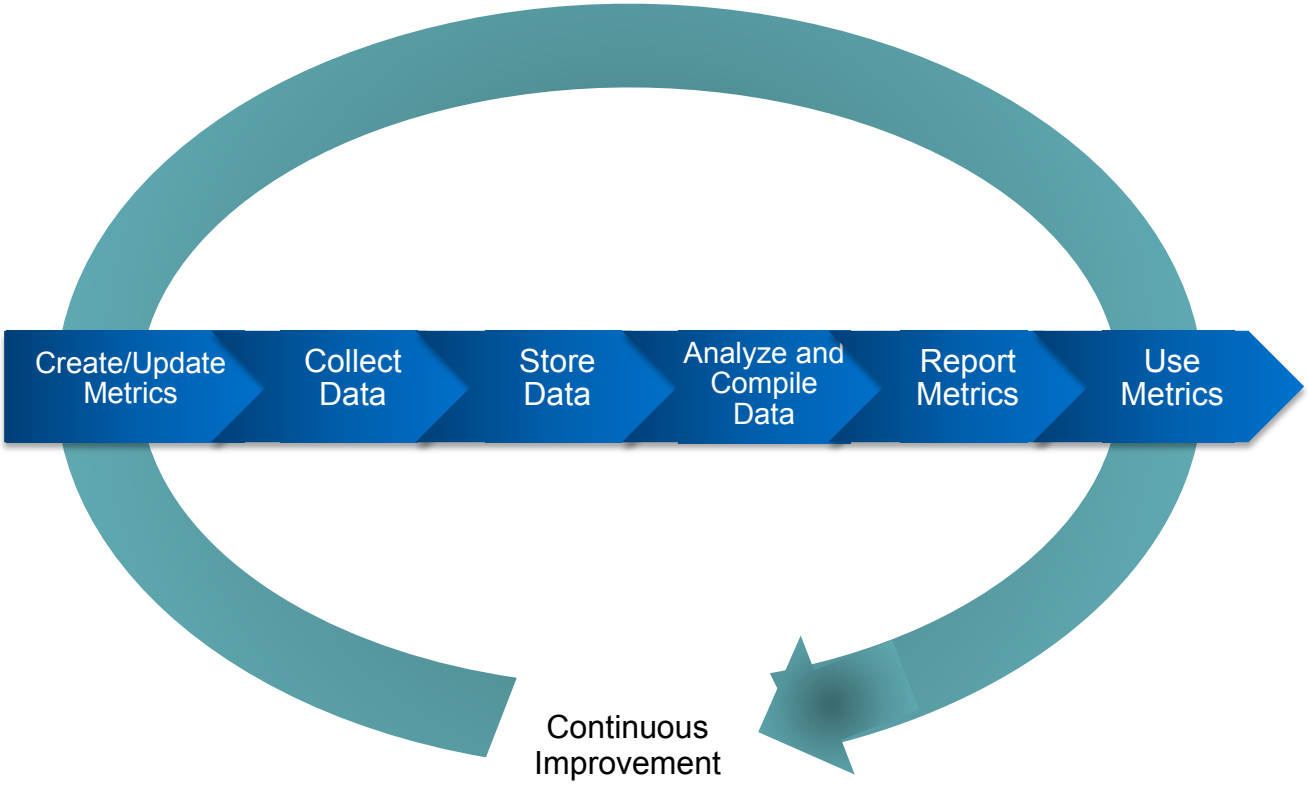

Figure 3-2
Basic Metrics Implementation Process[3]

[3] *Source:* Practical Measurement Framework for Software Assurance and Information Assurance, Version 1.0 *[2]*

While this process is generic enough to apply to any organization, there are special considerations for utilities regarding implementation, including:

- Data for OT systems may be processed manually due to their deterministic nature. In such cases, utilities must ensure that there are adequate resources for measurement in the OT environment.
- If metrics are collected for CIP regulated BES Cyber Systems, there must be additional protections on storing the raw data and any derivative metrics. Security teams should consult with their internal CIP auditing professionals.
- Utilities should adapt metrics used for reliability and safety for strategic level impacts to enterprise risk.

Any security metrics program will need to be supported by management and have adequate resources. Due to constraints across business units, one full-time employee with additional security or data science duties may only be able to manage 5-10 metrics. Thus, size and scope of the program will be important to future success. Moreover, management should be aware of the potential for unintended consequences of a metrics program, including:

- **New visibility**: Measuring parts of a security program for the first time will show gaps not previously encountered. Akin to installing a new intrusion detection system (IDS)— security teams will have visibility into data, trends, and indicators may that show a poorer performance than what was previously assumed. For example, a utility that does not measure the average mean time for discovering incidents may think that the number will be acceptable. However, once data is collected and analyzed, the mean may be higher than the target value.

  Implementing metrics will provide data that may be used to assess the security practices in a security program. As utilities begin to quantify and correlate more data to support security initiatives, changes in security practices, procedures, and technical controls should be based on these metrics. As a result, the metrics should reflect improvements in the cyber security program. However, initially there should be little expectation for managers or practitioners that new security metrics will support preconceived notions. The purpose of measuring is to *understand*, not assume, the effectiveness of a security program and the link to risk management.
- **Retirement of ineffective security metrics**: Since security metrics are relatively new, and not just in the electric sector, managers and practitioners should expect to learn what works and what does not work through trial and error in their metrics reporting. If, after a defined period (quarter, year, etc.), a metric does not prove to be useful, there should be a method to retire that metric and develop new security metrics.

As utilities become more dependent on projects that require metrics, such as Integrated Security Operations Centers (ISOCs) and the creation of cyber security architectures, it is important to leverage common lexicon and resources where appropriate. Since these projects will benefit the awareness and mitigation of cyber security risk in a utility's environment, it is imperative that managers and executives understand the value metrics can have in their organization.

4
SECURITY METRICS

While measurement and scientific observation are mature fields, there are still plenty of concepts to explore in applying those fields to cyber security in the electric sector. A set of metrics were developed and a set of data points were identified for metrics calculations as the starting point. The metrics are categorized into three different levels of hierarchical structure: strategic level, tactical level, and operational level. In this sections, the list of metrics is introduced and the relationship illustrated between the different levels of metrics.

Hierarchical Structure of Security Metrics

Illustrated in Figure 4-1 is the relationship between the three metric categories: strategic, tactical, and operational and some examples. At the highest level, there are three strategic metrics: Protection Score, Detection Score, and Response Score. These are executive-level summaries of the security status of an organization. The inputs for calculating strategic metrics are tactical and/or operational metrics. A tactical metric is an IT/OT management-level summary and calculated from various operational metrics. Operational metrics are at the lowest level in the metric hierarchy. They are measurements related to the day-to-day security operations activities.

To create a set of data-driven, quantitative metrics, various measurements must be collected from different parts of the information systems network. In this report, these measurements are defined as data points. Data points are the source for all metrics calculations in all three levels.

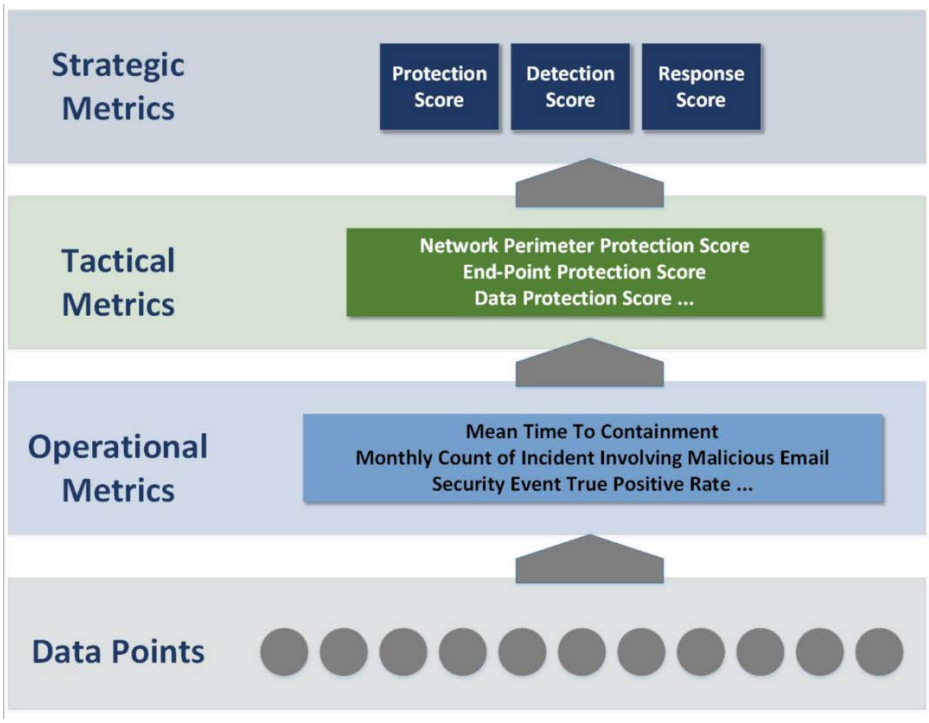

Figure 4-1
Hierarchy of Metrics

Metric Identifier and Naming Scheme

For ease of reference, a metric identifier scheme has been devised. Figure 4-2 illustrates the scheme, where the first letter stands for the metric level: Strategic, Tactical, or Operational. The last letters are acronyms of the metric name, for example, RS stands for Response Score and NPPS stands for Network Perimeter Protection Score, and so on. For an Operational Metric, there is one more letter between the first letter and the acronym. This letter identifies a "measurement category" that signifies the category of measurements or data points primarily used in the derivation of the metric. There are ten categories and they are listed in Table 4-1 below.

Table 4-1
Measurement Category

ID	Measurement Category
A	Asset
D	Database
E	Event Generating Device
I	Incident
M	Business Unit
N	Network Access Point
P	Person
T	Threat Alert
U	User
V	Vulnerability

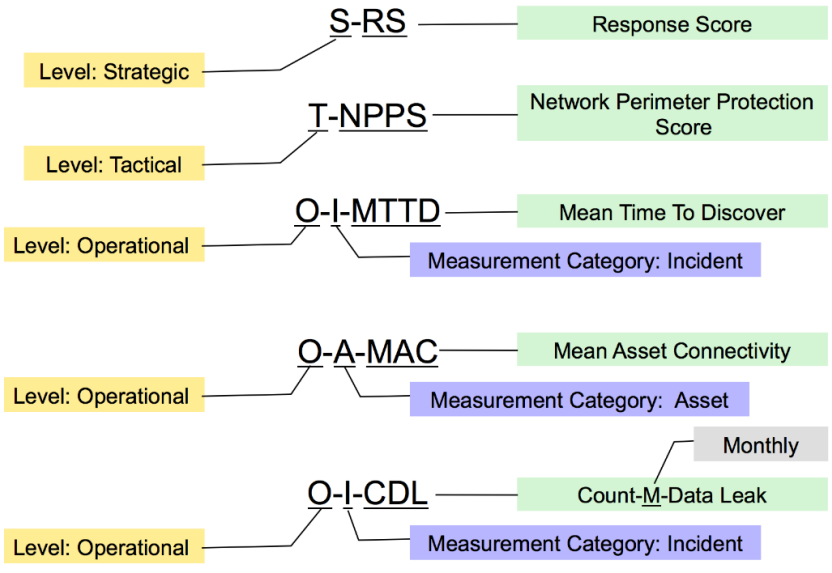

Figure 4-2
Metrics Identifier Naming Scheme

Strategic Metrics

Strategic Metrics are numerical representations of the security status in an organization at the highest level. They aim to indicate the overall effectiveness of corresponding controls in a target system. Three numbers - Protection Score, Detection Score and Response Score - are currently considered for Strategic Metrics. Higher value indicates better performance.

- Protection Score – a numerical value between 0 and 10, indicating the effectiveness of the overall protective controls in a target system.
- Detection Score – a numerical value between 0 and 10, indicating the effectiveness of the overall detective controls in a target system.
- Response Score – a numerical value between 0 and 10, indicating the effectiveness of the overall security incident response and recovery capability

The three Strategic Metrics loosely correspond to the core functions defined in the NIST Cybersecurity Framework [5]: Identify, Protect, Detect, Respond, and Recover. The reasons for not having one-to-one correlation with the core functions are because the primary objectives for strategic metrics and the NIST CSF are different.

1) The NIST CSF is a risk-based approach to managing cybersecurity risk. The objective is to apply the principles and best practices of risk management to improving the security and resilience of critical infrastructure. Therefore, it is comprehensive in coverage. Alternatively, security metrics aim to measure the result of the existing security program at a point in time. Therefore, only the controls and functions that are measurable and have direct impact to the state of security in a system are considered.

2) Activities for incident response and recovery often occur back-to-back and can be tracked together in a same system. After the exclusion of policy-oriented or process-centric functions from the NIST CSF, the measurements for response and recovery are consistent enough to be consolidated into one strategic metric, Response Score.

The primary inputs for calculating Strategic Metrics are Tactical Metrics. Table 4-2 below shows the associated Tactical Metrics for each Strategic Metric. The input metrics are subject to change based on further research. In particular, there are some differences in opinion regarding the right place for Security Management Score (denoted with an * in Table 4-2) and these differences are expected to be resolved with further discussion.

Table 4-2
Strategic Metrics and Associated Tactical Metrics

Metric ID	Strategic Metric	Tactical Metric ID	Tactical Metric Name
S-PS	Protection Score	T-NPPS	Network Perimeter Protection Score
		T-EPS	End-point Protection Score
		T-PAS	Physical Access Control Score
		T-HSS	Human Security Score
		T-NVS	Core Network Vulnerability Control Score
		T-NAS	Core Network Access Control Score
		T-DPS	Data Protection Score
		O-I-MTBI	Mean Time Between Security Incidents
		T-SMS-P	Security Management Score -Protection*
S-DS	Detection Score	T-TAS	Threat Awareness Score
		T-TDS	Threat Detection Score
		T-SMS-D	Security Management Score - Detection*
S-RS	Response Score	T-IRS	Incident Response Score
		T-SMS-R	Security Management Score - Response*

Tactical Metrics

Tactical Metrics are numerical representations of security status in an organization at the management level. They aim to indicate the overall effectiveness of tactical controls in a target system. There are eleven Tactical Metrics currently under review. A higher value of a metric indicates better performance.

- Network Perimeter Protection Score – a numerical value between 0 and 10, indicating the effectiveness of network perimeter protection controls. The security controls in place for perimeter protection are measured and balanced with the risk level associated with a network perimeter. These are the controls on network access points (wired or wireless), and for internet traffic through the perimeter (http proxy, email filter, etc.)
- End-point Protection Score – a numerical value between 0 and 10, indicating the effectiveness of end-point device protection controls. The security controls in place for end-point protection for both stationary and mobile end-points are measured and balanced with the risk level associated with the end-point. The controls include anti-malware protection, mobile device management, and host-based intrusion detection/prevention system.
- Physical Access Control Score – a numerical value between 0 and 10, indicating the effectiveness of physical access controls. The security controls in place for physical access control are measured and balanced with the risk level associated with the asset or a group of assets. The number of people with physical access, access authorization, and physical barriers in place to prevent unauthorized access are among the considerations.

- Human Security Score – a numerical value between 0 and 10, indicating the effectiveness of the human security component. The considerations include the frequency and completeness of security awareness training, phishing test performance, number of incidents involving social engineering, and number of incidents first detected by employees or other personnel.
- Core Network Vulnerability Control Score – a numerical value between 0 and 10, indicating the vulnerability control in a network. The risk of a vulnerability is calculated with the respect to the network connectivity and proximity and inverted to produce the control score. This metric captures the security of network design and effectiveness of system patching.
- Core Network Access Control Score – a numerical value between 0 and 10, indicating the effectiveness of access control in a network. The status of access control is calculated with respect to the network connectivity and proximity, capturing the controls in place through network design as well as access control to a specific device.
- Data Protection Score – a numerical value between 0 and 10, indicating the effectiveness of data protection in a network. This is a mean value of confidentiality score, availability score, and integrity score of all databases in the network.
- Security Management Score – a numerical value between 0 and 10, indicating the magnitude of security investment relative to the size of the system and the risk tolerance of the organization. This score can be separated into three different numbers proportionally to protection controls, detection controls, and response controls.
- Threat Awareness Score – a numerical value between 0 and 10, indicating the numerical the level of situational awareness and effectiveness of threat intelligence management.
- Threat Detection Score – a numerical value between 0 and 10, indicating the effectiveness of threat detection in both technical and procedural perspectives. This score relies on the accuracy of security event tracking and incident response data.
- Incident Response Score - numerical value indicating the effectiveness of the incident response program. This score relies on the accuracy of incident response/tracking data.

Table 4-3 below shows the input (Operational) metrics for each Tactical Metric. The input metrics are still draft and subject to change as the project progresses.

Table 4-3
Tactical Metrics and Associated Operational Metrics

Metric ID	Tactical Metric Name	Operational Metric ID	Operational Metric Name
T-NPS	Network Perimeter Protection Score	O-N-MAPS	Mean Access Point Protection Score
		O-N-MWAPS	Mean Wireless Access Point Protection Score
		O-N-MIPS	Mean Internet Traffic Protection Score
		O-I-MCME	Mean Count-M Malicious Email
		O-I-MCMU	Mean Count-M Malicious URL
		O-I-MCNP	Mean Count-M Network Penetration

Table 4-3 (continued)
Protection Strategic Metric and Associated Operational Metrics

Metric ID	Tactical Metric Name	Operational Metric ID	Operational Metric Name
T-EPS	End-point Protection Score	O-U-MSDPS	Mean Stationary End-Point Protection Score
		O-U-MMDPS	Mean Mobile End-Point Protection Score
		O-I-MCMW	Mean Count-M Malware
		O-I-MCMD	Mean Count-M Mobile End-Point
		O-I-MCSD	Mean Count-M Stationary End-Point
T-PAS	Physical Access Control Score	O-A-MPACS	Mean Physical Access Control Score
		O-I-MPAV	Mean Count-M Physical Access Violation
T-HSS	Human Security Score	O-H-MHSS	Mean Human Security Score
		O-I-MCSE	Mean Count-M Social Engineering
T-NVS	Core Network Vulnerability Control Score	O-A-MAC	Mean Asset Connectivity
		O-A-MAP	Mean Asset Proximity to Hostile Network
		O-A-MVRS	Mean Asset Vulnerability Risk Score
		O-A-MNVRS	Mean Network Vulnerability Risk Score
		O-I-MCNP	Mean Count-M Network Penetration
T-NAS	Core Network Access Control Score	O-A-MAC	Mean Asset Connectivity
		O-A-MAP	Mean Asset Proximity to Hostile Network
		O-A-MACS	Mean Asset Access Control Score
		O-A-MNACS	Mean Network Access Control Score
		O-I-MCNP	Mean Count-M Network Penetration
T-DPS	Data Protection Score	O-D-MDCS	Mean Data Confidentiality Score
		O-D-MDIS	Mean Data Integrity Score
		O-D-MDAS	Mean Data Availability Score
		O-I-MCDL	Mean Count-M Data Leak/Loss
T-SMS	Security Management Score	O-M-SBR	Security Budget Ratio
		O-M-SPR	Security Personnel Ratio
		O-M-CRTS	Cybersecurity Risk Tolerance Score

Table 4-3 (continued)
Protection Strategic Metric and Associated Operational Metrics

Metric ID	Tactical Metric Name	Operational Metric ID	Operational Metric Name
T-TAS	Threat Awareness Score	O-T-IES	Organization Threat Awareness Score
		O-T-MTIA	Mean Time from Intelligence to Action
		O-T-MTIP	Mean Time from Intelligence to Protection
		O-T-THES	Threat Hunting Effectiveness Score
T-TDS	Threat Detection Score	O-T-MITP	Mean Threat Intelligence True Positive Rate
		O-T-MCI	Mean Count-M Threat Intelligence
		O-E-METP	Mean Security Event True Positive Rate
		O-E-MC	Mean Count-D Security Events
		O-T-THTP	Mean Threat Hunting True Positive Rate
		O-T-MCH	Mean Count-M Threat Hunting Intelligence
		O-I-MCH	Mean Count-M High Severity Incidents
		O-I-MCM	Mean Count-M Medium Severity Incidents
		O-I-MCT	Mean Count-M Total Incidents
T-IRS	Incident Response Score	O-I-MTTD	Mean Time to Discovery
		O-I-MCMSI	Mean Count-M Missed Security Incidents
		O-E-SEMS	Security Event Management Score
		O-I-MTTC	Mean Time to Containment
		O-I-MTR	Mean Time to Recovery
		O-I-MTTA	Mean Time to First Action
		O-I-MCRM	Mean Cost of Response in Man-Hour (existing resource)
		O-I-MCRX	Mean Cost of Response in Dollar Amount (extra resource)

Operational Metrics

Operational Metrics are the lowest level metrics that are derived directly from the data points. They represent one specific aspect of security controls in a target system. Unlike Strategic or Tactical Metrics, Operational Metrics are not normalized into a numerical value between 0 and 10. There are currently 49 Operational Metrics being considered.

- Mean Asset Connectivity – an average Asset Connectivity of all assets in a target network. Asset Connectivity represents the degree of connectivity within a network. Generally higher asset connectivity is associated with higher risk.

- Mean Asset Access Control Score – an average Access Control Score of all assets in a target network. The Access Control Score is higher where there is a higher degree of controls preventing possible unauthorized access.
- Mean Asset Proximity to Hostile Network – an average Asset Proximity of all assets in a target network. Asset Proximity represents how close an asset is logically located to a hostile network. A lower proximity indicates higher risk.
- Mean Network Access Control Score – an average Network Access Control Score of all assets in a target network. This value represents the Asset Access Control Score augmented by the Asset Connectivity and Asset Proximity to Hostile Network. A Higher Network Access Control Score indicates a higher degree of control and lower risk.
- Mean Asset Vulnerability Risk Score – an average Asset Vulnerability Risk Score of all assets in a target network. The Asset Vulnerability Risk Score is the sum of the Common Vulnerability Scoring System (CVSS) of all vulnerabilities discovered in the asset. A high Asset Vulnerability Risk Score indicates high risk to the asset.
- Mean Network Vulnerability Risk Score – an average Network Vulnerability Risk Score of all assets in a target network. The Network Vulnerability Risk Score represents the Asset Vulnerability Risk Score adjusted by Asset Connectivity and Asset Proximity to the Hostile Network.
- Mean Physical Access Control Score – an average Physical Access Control Score of all assets in a network. The Physical Access Control Score represents the effectiveness of physical access controls for the asset.
- Mean Data Availability Score – an average Data Availability Score for all databases in a target network. The Data Availability Score represents the effectiveness of controls against data loss or unavailability for the database.
- Mean Data Confidentiality Score – an average Data Confidentiality Score for all databases in a target network. The Data Confidentiality Score represents the effectiveness of controls against the unauthorized disclosure of data stored in the database.
- Mean Data Integrity Score – an average Data Integrity Score for all databases in a target network. The Data Integrity Score represents the extent of controls against unauthorized or accidental modification of the data stored in the database.
- Mean Security Event True Positive Rate – an average value of True Positive Rate for all security event generating devices in a target network. The True Positive Rate is the number of security events that are confirmed as genuine security incidents over the number of all events generated by the device. A Higher True Positive Rate indicates higher accuracy.
- Mean Count-M Security Events – an average monthly count of all security events generated in a target network during last twelve months.
- Security Event Management Score – a numeric value indicating the effectiveness of security event management. The number of total security events generated, the degree of manual intervention, and correlation with external events are some of the factors for calculating this score.
- Mean Human Security Score – a numeric value indicating the effectiveness of security control involving human agents. Security awareness of individuals handling cyber assets and the security test results are considered in calculating this score.

- Mean Count-M Missed Security Incidents - an average monthly count of missed security incidents during the last twelve months. Missed security incidents include the incidents first noticed by malfunction of device, non-security staff report, compromise notification, adversary notification or public disclosure.
- Mean Count-M Data Leak/Loss – an average monthly count of security incidents involving data leak or loss during the last twelve months.
- Mean Count-M High Severity – an average monthly count of high severity security incidents during the last twelve months.
- Mean Count-M Medium Severity – an average monthly count of medium severity security incidents during the last twelve months.
- Mean Count-M Mobile End-Point – an average monthly count of security incidents involving mobile end-point during the last twelve months.
- Mean Count-M Malicious Email – an average monthly count of security incidents involving malicious email during the last twelve months.
- Mean Count-M Malicious URL – an average monthly count of security incidents involving malicious URL during the last twelve months.
- Mean Count-M Malware – an average monthly count of security incidents involving malware infection during the last twelve months.
- Mean Count-M Network Penetration– an average monthly count of security incidents involving network penetration during the last twelve months.
- Mean Count-M Stationary End-Point – an average monthly count of security incidents involving stationary end-point during the last twelve months.
- Mean Count-M Social Engineering – an average monthly count of security incidents involving social engineering during the last twelve months.
- Mean Count-M Physical Access Violation – an average monthly count of security incidents involving physical access violation during the last twelve months.
- Mean Count-M Total – an average monthly count of total security incidents during the last twelve months.
- Mean Time to Recovery – an average time in days from the discovery of an incident to the complete recovery from the incident.
- Mean Time to First Action – an average time in days from the discovery of an incident to the first action taken.
- Mean Time to Containment – an average time in days from the discovery of an incident to the containment of the incident.
- Mean Time to Discovery – an average time in days from the first occurrence of an incident to the first discovery of the incident. The day of first occurrence is usually found after the discovery through investigation.
- Mean Cost of Response in Man-Hour (existing resource) – an average cost of response in man-hours for existing resources normally engaged in incident response activities.
- Mean Cost of Response in Dollar Amount (extra resource) – an average cost of response in dollar amount for extra resources engaged in resolving a security incident.

- Cybersecurity Risk Tolerance Score – a numeric value representing the risk tolerance level of the organization. A Higher score indicates high tolerance to the risk.
- Security Budget Ratio – a ratio of the security budget over the total IT/OT budget.
- Security Personnel Ratio – a ratio of the number of full-time security personnel over the number of full-time IT/OT personnel.
- Mean Access Point Protection Score – an average Access Point Protection Score of all access points in a target network. The Access Protection Score must be calculated first for each access point from the numerical value representing security controls and risk associated with the access point.
- Mean Wireless Access Point Protection Score – an average Wireless Access Point Protection Score of all wireless access points in a target network. The Wireless Access Protection Score must be calculated first for each wireless access point from the numerical value representing security controls and risk associated with the wireless access point.
- Mean Internet Traffic Protection Score - an average Internet Traffic Protection Score of all internet traffic filtering devices in a target network. The score represents the extent of internet traffic controls in place such as DNS filtering, email filtering and web proxies.
- Organization Threat Awareness Score – a numerical value representing the threat/situational awareness of an organization. A high score indicates high awareness of security threats/risks.
- Mean Count-M Threat Intelligence – an average monthly count of threat intelligence received by an organization during the last twelve months.
- Mean Threat Intelligence True Positive Rate – an average value of True Positive Rate for all threat intelligence sources for an organization. The True Positive Rate is the number of threat intelligence warnings that are confirmed to lead to security incidents over the number of all threat intelligences generated by the source.
- Mean Time from Intelligence to Action – an average time in days from the day threat intelligence warning is received to the day the first action was taken by the receiving organization.
- Mean Time from Intelligence to Protection – an average time in days from the day threat intelligence warning is received to the day the organization completed the protective action.
- Threat Hunting Effectiveness Score – a numerical value indicating the effectiveness of threat hunting practices. A high score indicates a high degree of effectiveness.
- Mean Threat Hunting True Positive Rate – an average value of True Positive Rate for all threat hunting investigations occurring in a given period. The True Positive Rate is the number of threat hunting that lead to the discovery of security incidents over the number of all threat hunting investigations launched in the period.
- Mean Count-M Threat Hunting Investigation – an average monthly count of threat hunting investigations during the last twelve months.
- Mean Mobile End-Point Protection Score – a numerical value representing the effectiveness of security controls on the mobile end-point.
- Mean Stationary End-Point Protection Score – a numerical value representing the effectiveness of security controls on the stationary end-point.

Data Points

Security metrics calculations require repeatable data collected from various locations in a target network. 121 data points have been identified for collection and this preliminary list is included in Appendix B of this report.

5
DISCUSSION

Security metrics discussed in previous sections of this report are not intended to represent all aspects of security programs. Much confusion in developing the metrics can be avoided when the results of security controls are separated from the effort of implementing and maintaining them. Security metrics in this report aim to measure the results, not the efforts. Although this may sound discouraging, this separation is essential in producing objective and measurable numbers that reflect the security status as close as possible to the reality. Consequently, these numbers may be used to find out which of our effort worked and which did not, and gain further insights through trending and benchmarking.

Policies, processes, and/or technical controls exist to make the target system more secure. That is, they are to make the target system more difficult to be compromised and/or to stay compromised. Security metrics should give clear indication to this "security" of the target system. This is what is lacking in our industry and we are striving to achieve through this project.

Security policies and implementation procedures are components related to the maturity and sustainability of the security controls. One organization may have a high score in security metrics, but a poor result in a C2M2 assessment. Therefore, an organization must consider all four components of a cyber security program shown in Figure 2-1, and consider all three aspects - compliance, maturity, and effectiveness, when establishing a cyber security strategy.

6
NEXT STEPS

In 2015, EPRI examined security metrics research through existing literature and application to utility environments, including uses with the C2M2 and NERC CIP standards. That report represented the core components of a security metrics methodology. For security metrics to be successful across the electric sector, they must be used by multiple entities, regardless of size, function, or ownership structure. Following the initial publication in 2015, working sessions to review the metrics were conducted. Based on comments received, the methodology was revised in this 2016 version and a suite of security metrics were developed.

By having open dialogue on what metrics work, adapting existing measurement programs to accommodate cyber security, and encouraging information sharing with peers, the electric sector will benefit from mature dialogues across organizations and traditional boundaries. EPRI will continue to work with members and external partners on this important topic.

Topics for Future Research

Based on outreach with members and external partners, future research may include:

- Data collection strategies including specific IT and OT considerations on extracting data from manual sources
- Identification of security tools required for data collection
- Mapping of each metric to NERC CIP, the NIST CSF, and the C2M2
- Development of a methodology for rolling-up the lower level metrics to higher level metrics
- Normalization techniques for metric scores

In addition to finalizing the methodology, EPRI will work with members to pilot the methodology. Through the pilot program, the utilities will identify the best approach to adopting security metrics in alignment with their own organizational goals and risk management strategies.

EPRI will also work internally on tools and automated techniques, for members only, to implement various pieces of the security metrics methodology more effectively.

Finally, EPRI will continue the discussion among members and external partners to aggregate metrics for industry benchmarking.

7
WORKS CITED AND BIBLIOGRAPHY

[1] G. T. Doran, " There's a S.M.A.R.T. way to write management's goals and objectives," Management Review, p. 35–36, 1981.

[2] N. Bartol and et.al, "Practical Measurement Framework for Software Assurance and Information Assurance, Version 1.0," 1 October 2008. [Online]. Available: http://www.psmsc.com/Downloads/TechnologyPapers/SwA%20Measurement%2010-08-08.pdf. [Accessed 5 August 2015].

[3] E. Chew, M. Swanson, K. Stine, N. Bartol, A. Brown and W. Robinson, "NIST Special Publication 800-55, Rev. 1, Performance Measurement Guide for Information Security," National Institute of Standards and Technology, Gaithersburg, MD, 2008.

[4] Center for Internet Security, "The CIS Security Metrics," 1 November 2010. [Online]. Available: https://benchmarks.cisecurity.org/downloads/form/index.cfm?download=metrics.110. [Accessed 22 September 2015].

[5] National Institute of Standards and Technology (NIST), "Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0." (February 12, 2014).

Bibliography

International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC), “ISO/IEC 27004 Information technology – Security techniques - Information security management measurement.”

International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC), “ISO/IEC 15939, System and Software Engineering - Measurement Process.”

A. Jaquith, *Security Metrics: Replacing Fear, Uncertainty, and Doubt*, 5 April 2007. Addison-Wesley Professional.

U.S. Department of Energy, “Electricity Subsector Cybersecurity Capability Maturity Model,” February 2014. [Online]. Available: http://energy.gov/sites/prod/files/2014/02/f7/ES-C2M2-v1-1-Feb2014.pdf [Accessed 1 July 2015]

8
GLOSSARY

APPA	American Public Power Association
BES	Bulk Electric System
C2M2	Cybersecurity Capability Maturity Model
CIP	Critical Infrastructure Protection
COP	Common Operating Picture
CSF	Cybersecurity Framework
CVSS	Common Vulnerability Scoring System
DHS	Department of Homeland Security
DOD	Department of Defense
DOE	Department of Energy
EEI	Edison Electric Institute
ES-C2M2	Electricity Subsector Cybersecurity Capability Maturity Model
FISMA	Federal Information Security Management Act
ICS	Industrial Control Systems
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
ISO	International Organization for Standardization
ISOC	Integrated Security Operations Center
IT	Information Technology
MIL	Maturity Indicator Level
NERC	North American Electric Reliability Corporation
NESCOR	National Electric Sector Cybersecurity Organization Resource
NIST	National Institute of Standards and Technology
NISTIR	NIST Interagency Report

OT	Operations Technology
RMP	Risk Management Process
SP	Special Publication

A
METRICS TEMPLATE AND EXAMPLES

As discussed throughout this document, security metrics need to be adequately documented to ensure they are repeatable, transparent, and understandable. A template should be used to align terminology across a metrics and risk management program for cyber security. The template below can and should be edited to fit an organization's needs, which may or may not include objectives for the C2M2 or NIST Cybersecurity Framework (CSF). The metrics template, provided in Table A-1 should be tailored to fit the risk management objectives within a utility. [3]

(Note: the underlined fields are not in the NIST SP 800-55 template.)

Table A-1
Metrics Development Template

Field	Description
Metric ID	The unique identifier used for metric tracking and sorting. This unique identifier can be from an organization-specific naming convention or can directly reference another source.
Goal	Statement of strategic goal and/or cyber security goal. The goal should be based on an established hypothesis for the usefulness and impact for tracking this metric. This may cover programmatic goals or system-level goals, depending on the metric.
Supporting Framework Objective	If the organization is supporting or utilizing the NIST CSF or DOE C2M2, then the metrics template should incorporate either the CSF sub/category or C2M2 practice/objective being examined with the metric ID. Other, more general frameworks, such as the Network and Information Security (NIS) directive can also be used. This will help ensure the metrics program is aligned to existing terminology and program improvements.
Metric	Statement of metric. Use a numeric statement that begins with the word "percentage," "number," "frequency," "average," or a similar term.

Type	Statement of metric type (either implementation, effectiveness/efficiency, or impact).
	• *Implementation metrics* answer the question, "Is this program, procedures, policies, or activity being implemented?"
	• *Effectiveness/Efficiency metrics* answer the question, "Are the programs, procedures, policies, and activities implemented correctly, operating as intended, and meeting the desired outcome?" and may use previous implementation metrics.
	  o *Effectiveness* addresses the robustness of the result.
	  o *Efficiency* is related to timeliness of the result.
	• *Impact metrics* answer the question, "What mission-related benefits (or costs) are associated with the program, procedures, policies, or activities?"

Environment	Statement of where the metric is being measured. Due to the vastly different systems, architectures, and operating environments found at a utility, this should include differentiation between IT/OT and facilities (generation, transmission, distribution, and/or enterprise, as appropriate).
Formula	Calculation to be performed that results in a numeric expression of the metric. The information gathered serves as input into the formula for calculating the metric.

Table A-1 (continued)
Metrics Development Template

Field	Description
Target	Threshold for a satisfactory rating for the metric, such as milestone completion or a statistical metric. Target can be expressed in percentages, time, dollars, or other appropriate units of measure. Target may be tied to a required completion time frame. Select final and interim target to enable tracking of progress toward stated goal. There may be multiple targets for each IT/OT or facilities environment. Alternatively, some metrics may just be a reported value, or even binary, so a target field may not be necessary.
Applicable Standards and Requirements	Standards that may be used as references for controls or other information that may be needed for either the metric formula or tying back to the enterprise security program.
Frequency	Indication of how often the data is collected and analyzed, and how often the data is reported. Select the frequency of data reporting based on external reporting requirements and internal customer preferences.
Responsible Parties	Indicate the following key stakeholders: • Information Owner: Identify organizational component and role that owns required pieces of information; • Information Collector: Identify the organizational component and role responsible for collecting the data. (Note: If possible, Information Collector should be a different individual or even a representative of a different organizational unit than the Information Owner, to avoid the possibility of conflict of interest and ensure separation of duties. Smaller organizations will need to determine whether it is feasible to separate these two responsibilities.); and • Information Customer: Identify the organizational component and role who will receive the data.
Data Source	Location of the data to be used, automated or manual, in calculating the metric. Include databases, tracking tools, organizations, or specific roles within organizations that can provide required information. Should not be limited to just security-centric data, as information technology reliability statistics may be used.
Reporting Format	Indication of how the measure will be reported, such as a simple line chart or table, or more complex stacked bar charts, quartile time series charts, or different matrices. State the type of format or provide a sample.

Example Security Metrics

This section includes sample metrics with the template completed. The example metrics combined the template from NIST SP 800-55 with several discussion topics from the *CIS Security Metrics 2010* guidance. [4]

These example metrics align with objectives in both the NIST CSF, as well as the C2M2. While each organization will need to tailor metrics to their own risk management purposes, the foundational elements should aid utilities in their decision making process to adopt new metrics.

Table A-2
Example Metric 1: Incidents Requiring Manual Cleanup

Field	Description
Metric ID	**Incident Response 1**
Goal	Demonstrate the relative level of manual effort required to cleanup systems after virus detection.
Supporting Framework Objectives	NIST CSF Category: Analysis (RS.AN) and Mitigation (RS.MI) C2M2 Objective: • Reduce Cybersecurity Vulnerabilities (TVM-2) • Respond to Incidents and Escalated Cybersecurity Events (IR-3)
Metric	Number or percent of virus incidents that require manual clean up, compared to an overall total of viruses detected in user files: • By business unit • By facility, system, user, or device type
Type	Effectiveness/Efficiency
Environment	This metric can be measured where antivirus software and ticketing systems are used, primarily in enterprise environments, but also in certain OT facilities, including generation sites.
Formula	$\frac{Number\ of\ Virus\ Incidents\ Requiring\ Manual\ Cleanup}{Total\ Number\ of\ Viruses\ Detected} \times 100$
Target	This should be a low percentage, as designated by the organization.
Applicable Standards and Requirements	CIP-007-5 R3.1, NISTIR 7628 SG.RA-6, SG.IR-9, ISO/IEC 27001:2013 A.16, ISA/IEC 62443-2-1:2009 4.3.4.5
Frequency	Collection Frequency: Organization-defined (example: quarterly) Reporting Frequency: Organization-defined (example: quarterly)
Responsible Parties	• Information Owner: Chief Information Officer, Chief/Senior Information Security Officer or Business Unit Manager • Information Collector: System Administrator (by business unit or facility) • Information Customer: Chief Information Officer, Chief/Senior Information Security Officer
Data Source	Antivirus software, trouble-ticketing system, manual sources.
Reporting Format	Stacked bar chart illustrating the percentage of manual cleanup closed within targeted time frames over several reporting periods.

Table A-3
Example Metric 2: Mean-Time-to-Fix (MTTF)

Field	Description
Metric ID	**Incident Response 2**
Goal	Measure the effectiveness of an organization or business unit to recover from incidents.
Supporting Framework Objectives	NIST CSF Categories: Analysis (RS.AN) and Mitigation (RS.MI) C2M2 Objectives: • Detect Cybersecurity Events (IR-1) • Escalate Cybersecurity Events and Declare Incidents (IR-2) • Respond to Incidents and Escalated Cybersecurity Events (IR-3)
Metric	Number of hours per incident from when an incident occurs to recovery: • By business unit • By facility
Type	Effectiveness/Efficiency
Environment	Since dates of occurrence and dates of recovery can be tracked manually, MTTF can be measured in either IT or OT environments.
Formula	$\frac{\sum(Date\ of\ Recovery\ -\ Date\ of\ Occurrence)}{Total\ Number\ of\ Incidents}$
Target	MTTF values should trend lower over time.
Applicable Standards and Requirements	CIP-008-5 R1 and R2.3, NISTIR 7628 SG.IR-1, SG.IR-5 and SG.IR-6, ISO/IEC 27001:2013 A.12, A1.16.1.5, ISA/IEC 62443-2-1:2009 4.3.4.5, ISA 62443-3-3:2013 SR 6.1
Frequency	Collection Frequency: Organization-defined (example: quarterly) Reporting Frequency: Organization-defined (example: quarterly)
Responsible Parties	• Information Owner: Chief Information Officer, Chief/Senior Information Security Officer • Information Collector: System Administrator (by business unit or facility) • Information Customer: Chief Information Officer, Chief/Senior Information Security Officer
Data Source	Security incident and event management (SIEM) systems, host logs, antivirus software, trouble-ticketing system, manual sources.
Reporting Format	Bar chart of Time (week, month, quarter) versus MTTF (hours per incident)

Table A-4
Example Metric 3: Cyber Security Workforce Skills

Field	Description
Metric ID	**Workforce Management 1**
Goal	Demonstrate the relative level of security expertise recruited by the organization, within the security team and throughout the enterprise.
Supporting Framework Objectives	NIST CSF Category: Asset Management (ID.AM-6) C2M2 Objective: Assign Cybersecurity Responsibilities (WM-1)
Metric	Number or percent of position descriptions defining cyber security roles, responsibilities, skills, and certifications: • By business unit • By facility • By role, skill, certification, etc.
Type	Implementation
Environment	This metric can be measured across an organization, regardless of environment
Formula	$\frac{Number\ of\ Postion\ Descriptions\ with\ definited\ security\ roles, etc.}{Total\ Number\ of\ Position\ Descriptions} \times 100$
Target	As designated by the organization, based on risk analysis.
Applicable Standards and Requirements	ISA 62443-2-1:2009 4.3.2.3, ISO/IEC 27001:2013 A.6.1.1
Frequency	Collection Frequency: Organization-defined (example: annually) Reporting Frequency: Organization-defined (example: annually)
Responsible Parties	• Information Owner: Human Resources Director (or equivalent) • Information Collector: Organization-defined • Information Customer: Chief Information Officer, Chief/Senior Information Security Officer
Data Source	Human resources management software, manual sources.
Reporting Format	Stacked bar chart of total number of positions, with a breakdown of roles and responsibilities, by business unit or security team.

Table A-5
Example Metric 4: Mean Cost (or Hours Spent) to Mitigate Vulnerabilities

Field	Description
Metric ID	**Vulnerability Management 1**
Goal	Understand the relative level of effort required to mitigate vulnerabilities across different business units and facilities. Since cost may be difficult, hours spent can originally be used and defined.
Supporting Framework Objectives	NIST CSF Category: Analysis (RS.AN) and Mitigation (RS.MI) C2M2 Objective: Reduce Cybersecurity Vulnerabilities (TVM-2)
Metric	Average (mean) US dollars/Euros or hours spent for the organization to mitigate identified vulnerabilities: • By business unit • By facility
Type	Impact
Environment	Since hours and costs can be tracked manually, this metric can be measured in either IT or OT environments.
Formula	$\frac{\sum((Person\ Hours\ to\ Mitigate\ \times\ Hourly\ Rate) + Other\ Mitigation\ Costs)}{Total\ Number\ of\ Mitigated\ Vulnerabilities}$
Target	In IT environments, vulnerabilities will ideally be handled by automated remediation systems, so the cost should be near or equal to zero. However, due to the complexities of different systems, especially in OT and compliance spaces, this cost may be understandably higher.
Applicable Standards and Requirements	N/A
Frequency	Collection Frequency: Organization-defined (example: monthly) Reporting Frequency: Organization-defined (example: monthly)
Responsible Parties	• Information Owner: Chief Information Officer, Chief/Senior Information Security Officer • Information Collector: System Administrator (by business unit or facility) • Information Customer: Chief Information Officer, Chief/Senior Information Security Officer
Data Source	Manual sources, budget resources, trouble-ticketing systems
Reporting Format	Bar chart of Time (week, month, quarter) versus Mean cost (or hours) to Mitigate Vulnerabilities ($)

Table A-6
Example Metric 5: Percent of Changes with Security Review

Field	Description
Metric ID	**Change Management 1**
Goal	Demonstrate the level of security considered for all change and configuration management practices across the organization
Supporting Framework Objectives	NIST CSF Category: Information Protection Processes and Procedures (PR.IP) C2M2 Objective: Manage Changes to Assets (ACM-3)
Metric	Percent of system or configuration changes reviewed for security impacts prior to implementation.
Type	Implementation
Environment	This metric can be measured where antivirus software and ticketing systems are used, primarily in enterprise environments, but also in certain OT environments.
Formula	$\frac{Number\ of\ Completed\ Changes\ with\ a\ Security\ Review}{Total\ Number\ of\ Completed\ Changes} \times 100$
Target	This percentage should trend higher over time as most, if not all, changes to systems and configurations should include a review of security impacts.
Applicable Standards and Requirements	CIP-010-1 R1, NISTIR 7628 SG.CM-1, SG.CM-4, ISA 62443-2-1:2009 4.3.4.3.2, 4.3.4.3.3, ISA 62443-3-3:2013 SR 7.6, ISO/IEC 27001:2013 A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4
Frequency	Collection Frequency: Organization-defined (example: quarterly) Reporting Frequency: Organization-defined (example: quarterly)
Responsible Parties	• Information Owner: Chief Information Officer, Chief/Senior Information Security Officer • Information Collector: System Administrator • Information Customer: Chief Information Officer, Chief/Senior Information Security Officer
Data Source	Configuration management software, trouble-ticketing system, manual sources.
Reporting Format	Bar chart of time (organization-defined frequency or other) versus Percent of Changes with Security Review values.

B
DATA POINTS

Following is the preliminary set of data points that may be used as input to the operational metrics. Included with each data point is a Measurement Category Identifier that is used to indicate the data source category.

Table B-1
Data Points

Data Point ID	Data Point	Collection Scope	Data Type	
A01	Number of internal IPs reachable	Per Asset	Integer	
A02	Outbound connection to internet	Per Asset	Yes/No	
A03	Inbound connection from the internet	Per Asset	Yes/No	
A08	Asset Criticality Rating	Per Asset	Integer	
A09	Number of active default account/password	Per Asset	Integer	
A10	Number of active system-privileged accounts	Per Asset	Integer	
A11	Number of active shared accounts (shared password or no password)	Per Asset	Integer	
A15	Number of total users who can login to the system	Per Asset	Integer	
A16	Number of total users who are authorized to login to the system	Per Asset	Integer	
A17	Number of people who are authorized to access the asset (can touch)	Per Asset	Integer	
A18	Number of people who can access the asset without force (can touch)	Per Asset	Integer	
A19	Number of physical barriers to the asset from the closest public location	Per Asset	Integer	
D01	Data Criticality Rating (Confidentiality, Integrity, Availability)	Per Database	Category	Low, Medium, High
D02	Encryption at rest	Per Database	Yes/No	
D03	Encryption in transit	Per Database	Yes/No	
D06	Data Redundancy	Per Database	Integer	
D07	Backup Frequency	Per Database	Category	On Change, Hourly, Daily, Weekly, Monthly

Table B-1 (continued)
Data Points

Data Point ID	Data Point	Collection Scope	Data Type	
E01	Number of events generated by SIEM/IDS/IPS per day	Per SIEM/IDS/IPS	Integer	
E02	Number of events requires manual intervention per day	Per SIEM/IDS/IPS	Integer	
E03	Correlation with external intelligence	Per SIEM/IDS/IPS	Yes/No	
E04	Number of confirmed security incidents detected by this device per month	Per SIEM/IDS/IPS	Integer	
I01	Date first noticed	Per Incident	Date	
I02	Date of first occurrence	Per Incident	Date	
I04	Date first actioned	Per Incident	Date	
I05	Date contained	Per Incident	Date	
I06	Date completed mitigation	Per Incident	Date	
I07	Network penetration involved	Per Incident	Yes/No	
I08	Data leak/loss involved	Per Incident	Yes/No	
I09	Social engineering involved	Per Incident	Yes/No	
I10	Malware involved	Per Incident	Yes/No	
I11	Mobile End-Point	Per Incident	Yes/No	
I12	Malicious Email involved	Per Incident	Yes/No	
I13	Malicious URL involved	Per Incident	Yes/No	
I14	Physical access violation involved	Per Incident	Yes/No	
I15	Severity rating	Per Incident	Category	Low, Medium, High
I16	Cost of response in man-hour (existing resources)	Per Incident	Real	
I17	Cost of response in dollar amount (extra resources)	Per Incident	Real	

Table B-1 (continued)
Data Points

Data Point ID	Data Point	Collection Scope	Data Type	
I18	First detected by employee report	Per Incident	Yes/No	
I19	First noticed by external compromise notification	Per Incident	Yes/No	
I20	First noticed by malfunction of resource	Per Incident	Yes/No	
I21	First noticed by alert generated by security software/hardware	Per Incident	Yes/No	
I22	First noticed by threat hunting	Per Incident	Yes/No	
I23	First noticed by investigation of external threat intelligence	Per Incident	Yes/No	
M01	Annual IT/OT Budget	Per Business Unit	Real	
M02	Annual Security Budget	Per Business Unit	Real	
M03	Number of IT/OT full-time staffs	Per Business Unit	Integer	
M04	Number of Security full-time staffs	Per Business Unit	Integer	
M05	Number of total active security exceptions	Per Business Unit	Integer	
M06	Level of final approval for security exceptions	Per Business Unit	Category	Executive, Director, Manager, Senior Staff, Junior Staff
M07	Level of highest full-time security personnel	Per Business Unit	Category	Executive, Director, Manager, Senior Staff, Junior Staff
M08	Business Unit that the highest full-time security personnel reports to	Per Business Unit	Category	
N01	Number of inbound connections per day	Per Network Access Point	Integer	
N02	Number of outbound connections per day	Per Network Access Point	Integer	
N03	Number of dropped inbound connections per day	Per Network Access Point	Integer	

Table B-1 (continued)
Data Points

Data Point ID	Data Point	Collection Scope	Data Type	
N04	Number of all alerts per day	Per Network Access Point	Integer	
N05	Number of security alerts per day	Per Network Access Point	Integer	
N06	Number of probes per day	Per Network Access Point	Integer	
N07	Number of confirmed DOS attempts per month	Per Network Access Point	Integer	
N08	Number of confirmed intrusion attempts per month	Per Network Access Point	Integer	
N09	Number of confirmed cyber incidents that required human intervention per month	Per Network Access Point	Integer	
N10	Wireless communication allowed	Per Network Access Point	Yes/No	
N11	Wireless: Protocol	Per Network Access Point	Category	802.11a, 802.11b, 802.11g, 802.11n, 802.11ac, 802.11ad, other
N12	Wireless: Signal Strength in dBm	Per Network Access Point	Integer	
N13	Wireless: Encryption	Per Network Access Point	Category	WEP, WPA, WPA2-Preshared, WPA2-Enterprise, other
N14	Wireless: Antenna Type	Per Network Access Point	Category	Omni-directional, directional, point-to-point
N15	Wireless: FHSS (Frequency-hoping Spread Spectrum) or other anti-jamming protection	Per Network Access Point	Yes/No	
N16	Email: Number of total inbound emails per day	Per Email Server/Filter	Integer	
N17	Email: Number of total outbound emails per day	Per Email Server/Filter	Integer	
N18	Email: Number of filtered emails per day	Per Email Server/Filter	Integer	
N19	Email: Number of spams detected per week	Per Email Server/Filter	Integer	
N20	Email: Number of phishing attempts detected per week	Per Email Server/Filter	Integer	

Table B-1 (continued)
Data Points

Data Point ID	Data Point	Collection Scope	Data Type	
N21	Email: Number of malware detected per week	Per Email Server/Filter	Integer	
N22	Email: Number of spams reported by the user per week	Per Email Server/Filter	Integer	
N23	Email: Number of phishing attempts reported by the user per week	Per Email Server/Filter	Integer	
N24	Email: Number of malware reported by the user per week	Per Email Server/Filter	Integer	
N25	Email: Number of outbound email with sensitive data - detected	Per Email Server/Filter	Integer	
N26	Web Proxy: % of end-point going through proxy	Per Email Server/Filter	Real	
N27	Web Proxy: general social network sites allowed for all users	Per Email Server/Filter	Yes/No	
N28	Web Proxy: private email access allowed for all users	Per Email Server/Filter	Yes/No	
N29	Web Proxy: private cloud storage allowed for all users	Per Email Server/Filter	Yes/No	
P01	Last security awareness training	Per Personnel	Category	< 1 week, < 4 weeks, 3 months, > 3 months
P02	System-privileged access to at least one system	Per Personnel	Yes/No	
P03	Physical access to at least one cyber asset	Per Personnel	Yes/No	
P04	Read-access to at least one type of high criticality rating data	Per Personnel	Yes/No	
P05	Write-access to at least one type of high criticality rating data	Per Personnel	Yes/No	
P06	Business Unit ID	Per Personnel	Yes/No	

Table B-1 (continued)
Data Points

Data Point ID	Data Point	Collection Scope	Data Type	
P07	Total number of personnel	Per Business Unit	Integer	
P08	Number of personnel who participated in social engineering test	Per Business Unit	Integer	
P09	Failure rate on last email phishing test	Per Business Unit	Real	
T01	Number of organizations directly providing threat intelligence under contract/agreement	Per Business Unit	Integer	
T02	Number of organizations directly providing threat intelligence informally	Per Business Unit	Integer	
T03	Intelligence received from	Per warning/alert	Category	
T04	Date threat warning/alert received	Per warning/alert	Date	
T05	Date threat warning/alert reported to the highest accountable management	Per warning/alert	Date	
T06	Date threat warning/alert response action started	Per warning/alert	Date	
T07	Date threat warning/alert response completed	Per warning/alert	Date	
T08	Led to (a) confirmed security incident(s)	Per warning/alert	Yes/No	
T09	Threat hunting program	Per Business Unit	Yes/No	
T10	Number of employees trained for threat hunting	Per Business Unit	Integer	
T11	Number of threat hunting investigation per month	Per Business Unit	Real	
U01	Malware protection: Anti-virus signature update frequency	Per end-user device	Category	Min, Hour, Day, Week+
U02	Malware protection: Anti-virus scan frequency	Per end-user device	Category	On Access, Min, Hour, Day, Week+
U03	Malware protection: Number of applications that are exempt from anti-virus scan	Per end-user device	Integer	

Table B-1 (continued)
Data Points

Data Point ID	Data Point	Collection Scope	Data Type	
U04	Malware protection: Total size of files/folders/drives that are exempt from anti-virus scan	Per end-user device	Integer	
U05	Mobile device: Encryption	Per end-user device	Category	Mandatory, Discretionary, No Encryption
U06	Mobile device: Central management of device security policy	Per end-user device	Yes/No	
U07	Mobile device: Theft/Lost device control	Per end-user device	Yes/No	
U08	HIDS management	Per end-user device	Category	Mandatory, Discretionary, No Policy Management
U09	Number of connections to critical data/asset/application allowed from this device	Per end-user device	Integer	
V01	Vulnerability ID	Per Vulnerability	Text	
V02	Vulnerability CVSS	Per Vulnerability	Real	
V03	Asset ID	Per Vulnerability	Category	Organization Defined

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

3002007886

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