ELECTRIC POWER
RESEARCH INSTITUTE

Creating Security Metrics for the Electric Sector

3002005947

Creating Security Metrics for the Electric Sector

3002005947

Technical Update, December 2015

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 DOCUMENT WAS PREPARED BY THE ORGANIZATION(S) NAMED BELOW AS AN ACCOUNT OF WORK SPONSORED OR COSPONSORED BY THE ELECTRIC POWER RESEARCH INSTITUTE, INC. (EPRI). NEITHER EPRI, ANY MEMBER OF EPRI, ANY COSPONSOR, THE ORGANIZATION(S) BELOW, NOR ANY PERSON ACTING ON BEHALF OF ANY OF THEM:

(A) MAKES ANY WARRANTY OR REPRESENTATION WHATSOEVER, EXPRESS OR IMPLIED, (I) WITH RESPECT TO THE USE OF ANY INFORMATION, APPARATUS, METHOD, PROCESS, OR SIMILAR ITEM DISCLOSED IN THIS DOCUMENT, INCLUDING MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, OR (II) THAT SUCH USE DOES NOT INFRINGE ON OR INTERFERE WITH PRIVATELY OWNED RIGHTS, INCLUDING ANY PARTY'S INTELLECTUAL PROPERTY, OR (III) THAT THIS DOCUMENT IS SUITABLE TO ANY PARTICULAR USER'S CIRCUMSTANCE; OR

(B) ASSUMES RESPONSIBILITY FOR ANY DAMAGES OR OTHER LIABILITY WHATSOEVER (INCLUDING ANY CONSEQUENTIAL DAMAGES, EVEN IF EPRI OR ANY EPRI REPRESENTATIVE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES) RESULTING FROM YOUR SELECTION OR USE OF THIS DOCUMENT OR ANY INFORMATION, APPARATUS, METHOD, PROCESS, OR SIMILAR ITEM DISCLOSED IN THIS DOCUMENT.

REFERENCE HEREIN TO ANY SPECIFIC COMMERCIAL PRODUCT, PROCESS, OR SERVICE BY ITS TRADE NAME, TRADEMARK, MANUFACTURER, OR OTHERWISE, DOES NOT NECESSARILY CONSTITUTE OR IMPLY ITS ENDORSEMENT, RECOMMENDATION, OR FAVORING BY EPRI.

THE ELECTRIC POWER RESEARCH INSTITUTE (EPRI) PREPARED THIS REPORT.

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.

Electric Power Research Institute, EPRI, and TOGETHER…SHAPING THE FUTURE OF ELECTRICITY are registered service marks of the Electric Power Research Institute, Inc.

Copyright © 2015 Electric Power Research Institute, Inc. All rights reserved.

ACKNOWLEDGMENTS

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

Principal Investigator
J. Christopher

This report describes research sponsored by EPRI. EPRI would like to acknowledge the support of the following organizations:

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

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

Creating Security Metrics for the Electric Sector. EPRI, Palo Alto, CA: 2015. 3002005947.

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—including destroying, stealing, or compromising the availability and integrity of data. Although 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 security in a consistent way. Building on previous efforts, the electricity industry leverages various security metrics and is constantly maturing in this relatively new field.

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

Keywords

Cyber security
Cyber security metrics
Cyber security risk management
Information assurance

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

Creating Security Metrics for the Electric Sector. EPRI, Palo Alto, CA: 2015. 3002005947.

EXECUTIVE SUMMARY

Product ID: 3002005947

Creating Security Metrics for the Electric Sector

PRIMARY AUDIENCE: Cyber security practitioners

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

This document provides foundational information for further research on a security metrics methodology. It is based on literature reviews of previous cyber security research, as well as member and external partner outreach. Utilities have unique considerations for creating or updating a security metrics program. This 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 systems and the highly-specialized operations technology systems, including industrial control systems. These systems, which lack modern security capabilities, will not benefit from automated sources of data collection—a key step toward implementing security metrics. The foundational elements of this research outline the uses for metrics and leverage existing guidance for a basic metrics program. In addition, EPRI collaborated with members and external partners to create and vet a template for creating security metrics, as well as examples that can be leveraged for a new measurement program. Finally, next steps for creating a security metrics methodology are outlined for future research.

KEY FINDINGS

- Data will need to be collected across organizational boundaries and reported at various levels, including management and executives.
- Many existing efforts can complement a security metrics program, including mandatory regulations and voluntary adoption of security frameworks.
- Senior managers and executives must be engaged in the program before security metrics are established.
- Security metrics can supplement data needed for security architectures, integrated security operation centers, and common operating pictures.

VALUE STATEMENT

This research explains the steps needed to create a security metrics program, which can relate the allocation of people, processes, and tools to enterprise risk management. When implemented, a security metrics program would be similar to the way in which reliability and safety indices are reported throughout business units and with senior management.

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

Creating Security Metrics for the Electric Sector. EPRI, Palo Alto, CA: 2015. 3002005947.

HOW TO APPLY RESULTS
Any utility developing a security metrics program must engage with senior management and executives before creating the appropriate metrics. As a relatively new field, security metrics will not be as mature or robust as utility counterparts in finance, reliability operations, or safety. Therefore, security practitioners will need to set realistic expectations and establish a direct link to the enterprise risk management program. From there, the guidance in this document can be discussed and applied, with specific tailoring for security metrics and consideration of the metrics template and examples found in Appendix A and Appendix B.

EPRI CONTACTS: Annabelle Lee, Senior Technical Executive, 202.293.6345, alee@epri.com

© 2015 Electric Power Research Institute (EPRI), Inc. All rights reserved. Electric Power Research Institute, EPRI, and
TOGETHER...SHAPING THE FUTURE OF ELECTRICITY are registered service marks of the Electric Power Research Institute, Inc.

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 B).

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.

- **Measure:** Variable to which a value is assigned as the result of measurement [ISO/IEC 15939]
- **Measurement:** The process to determine a value [ISO 27004]

For the purposes of this document, a **metric** will use the same definition as a **measure**, which must be determined by a **measurement**. Metric will be used throughout this document.

Conceptually, it is important to realize that utilities can, and should, measure things at different levels of the organization, as seen below.

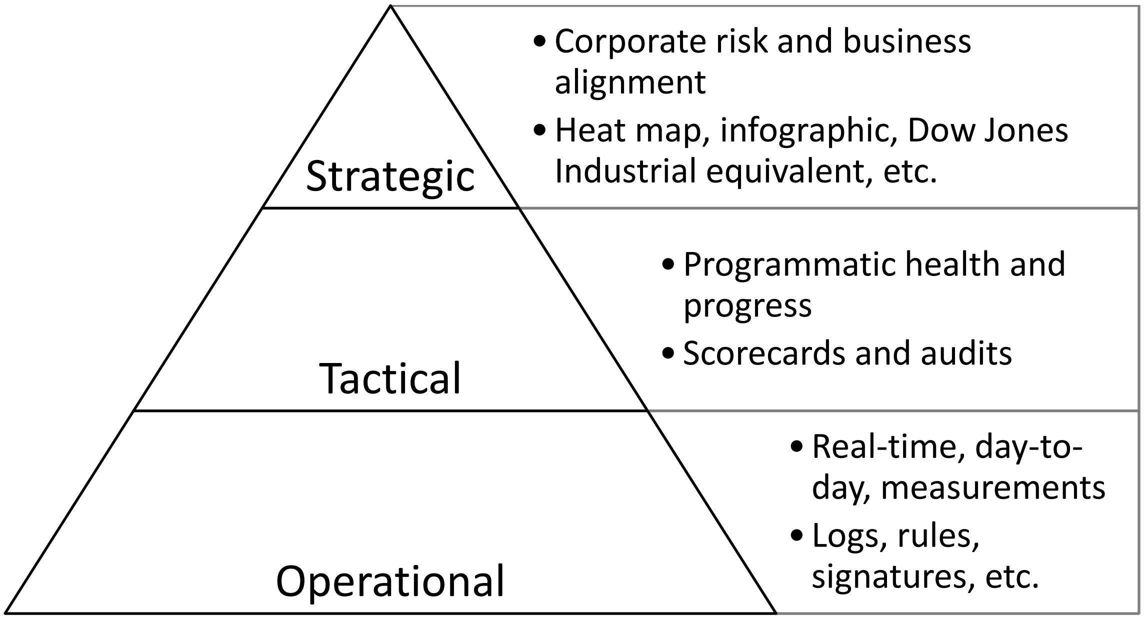
Strategic
• Corporate risk and business alignment
• Heat map, infographic, Dow Jones Industrial equivalent, etc.
Tactical
• Programmatic health and progress
• Scorecards and audits
Operational
• Real-time, day-to-day, measurements
• Logs, rules, signatures, etc.

Figure 1-1
Organizational levels and various measurement data

Each level of the organization, ranging from operational to strategic, will have useful sets of 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 data and metrics collected 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 extremely important, in today’s security environment, most executives want to know, “How secure are we?” This is not the same audience or reporting as the tactical metrics. Moreover, most security managers are challenged to summarize large volumes of technical data into infographics 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 the 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;
- 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, like finances 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.

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 (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 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, while able to provide a common taxonomy for discussing cyber security threats and vulnerabilities, detract the focus from process improvement towards compliance and adhering to recommended practices.

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 like 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 (C2M2). 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 C2M2 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.

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 mnemonic 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 National Institute of Standards and Technology (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 must 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, the National Institute of Standards and Technology (NIST) released Special Publication (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 measures 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 Templates and Examples

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 DOE 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 B. Also included are examples of operational-level security metrics.

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 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.

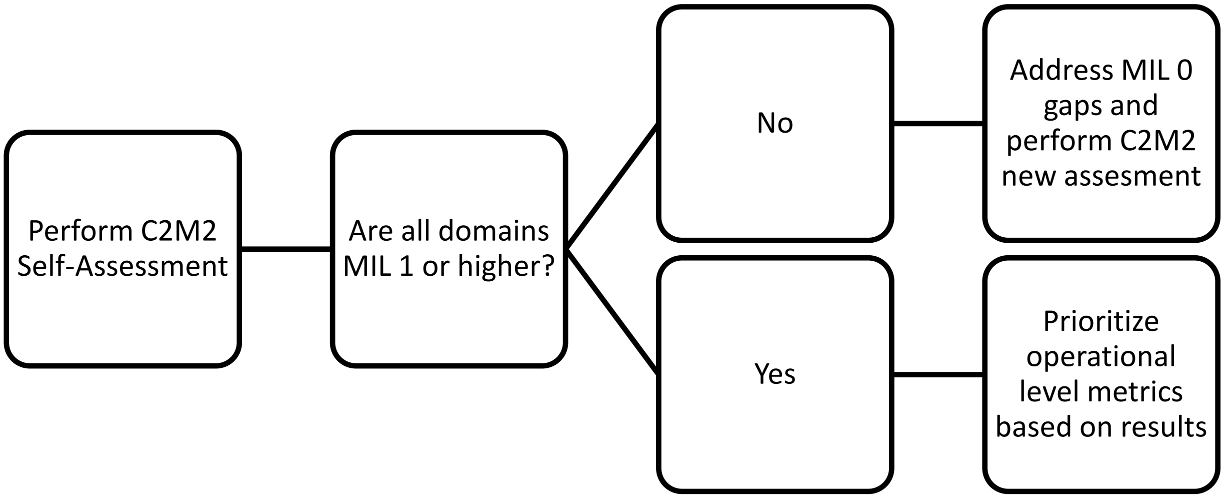
Perform C2M2 Self-Assessment
Are all domains MIL 1 or higher?
No
Yes
Address MIL 0 gaps and perform C2M2 new assesment
Prioritize operational level metrics based on results

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 have 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 measurement? Can data supporting those practices be collected through automated means?
- For practices that may be ad hoc in MIL 1, can measurements 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 example template in Appendix B 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 New 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 measures 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.

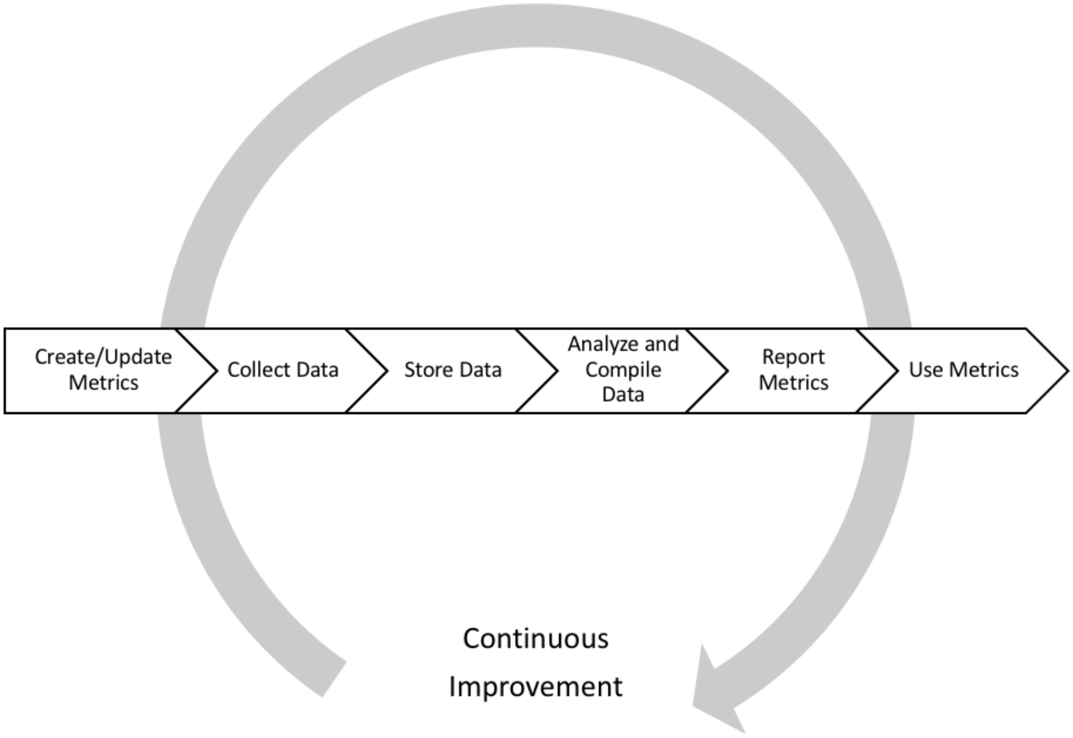

Figure 3-2
Basic metrics implementation process
Source: Practical Measurement Framework for Software Assurance and Information Assurance, Version 1.0 *[2]*

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 being 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 to discuss impacts to enterprise risk at the strategic level of Figure 1-1.

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 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 and data, trends, and indicators may show a poor performance compared to what was previously assumed. For example, a utility that does not measure its 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 high. Adding measurement is adding a new comprehension of the practices in any security program. As utilities begin to quantify and correlate more data to support security initiatives, these trends will improve, but 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 architecture documentation, it is important to leverage common lexicon and resources where appropriate. Since these projects will, ultimately, 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
NEXT STEPS

In 2015, EPRI and the partners of this report examined security metrics research through existing literature and application to utility environments, including uses with the C2M2 and NERC CIP Standards. The contents of this document represent the core components that will be released in a security metrics methodology later next year.

For security metrics to be successful across the electric sector, they must be used by multiple entities, regardless of size, function, or ownership structure. This report, and the subsequent methodology document in 2016, will be released publicly for the benefit of the sector and EPRI members. By having open dialogue on what metrics work, adapting existing measurement programs to accommodate cyber security, and encouraging information sharing with peers, our sector will benefit from mature dialogues across organizations and traditional boundaries. EPRI will continue to work with our members and external partners on this important topic.

Topics for Future Research

As already mentioned, the security metrics methodology will be finalized in 2016, along with a process diagram and actionable steps for creating a metrics program in the utility environment. Based on outreach with members and external partners, future research will include considerations for:

- Specific IT and OT considerations on pulling data from manual sources;
- Analysis and correlation techniques for actionable, risk-based observations on program capabilities and new security projects;
- Translation of operational data to strategic goals and risk management objectives, as outlined in Figure 1-1; and
- Establishment of common lexicon for security metrics, architecture, and Common Operating Pictures (COPs);

Once a methodology is developed, EPRI will test and pilot a security metrics program with volunteer utilities.

In addition to finalizing the methodology, EPRI will continue to work with members and external partners on the metrics template and actionable examples for use in IT and OT environments. This will continue to ensure that any utility, regardless of size, function, or ownership structure can update or create a security metrics program that align with their own organizational goals and risk management strategies.

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

5
REFERENCES

Works Cited

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, et al., "Practical Measurement Framework for Software Assurance and Information Assurance, Version 1.0," 1 October 2008. 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. . https://benchmarks.cisecurity.org/downloads/form/index.cfm?download=metrics.110. [Accessed 22 September 2015].

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."

Jaquith, A., *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]

A

ACRONYMS AND ABBREVIATIONS

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
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

B

NOTIONAL METRICS FOR CONSIDERATION

Using a Metrics Development Template

As discussed throughout this document, security metrics need to be adequately documented to ensure they are repeatable, transparent, and understandable. A template, like the example below, 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. The metrics template, provided in Table B-1, and the following examples, should be tailored to fit the risk management objectives within a utility. [3]

As mentioned in Section 4, the template and examples (Tables B-1 through B-6) are preliminary and EPRI is currently seeking comments on how to improve this content for use throughout the industry. In November 2015, member utilities and external partners provided feedback, which will be incorporated into future versions of the methodology and technical updates on security metrics research.

Table B-1
Metrics Development Template

Field	Data
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.
Organization 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 C2M2 and NIST CSF Objective	If the organization is supporting or utilizing the NIST Cybersecurity Framework or DOE/DHS C2M2, then the metrics template should incorporate either the CSF sub/category or C2M2 practice/objective being examined with the metric ID. This will help ensure the metrics program is aligned to existing terminology and program improvements.
Measurement	Statement of measurement. Use a numeric statement that begins with the word "percentage," "number," "frequency," "average," or a similar term.

Table B-1 (continued)
Metrics Development Template

Field	Data
Type	Statement of metric type (either implementation, effectiveness/efficiency, or impact). • *Implementation metrics* answer the question, “Is this practice, process, or activity being performed?” regardless of effectiveness or what contribution the activity may make to overall security improvements. • *Effectiveness/Efficiency metrics* answer the question, “How good is the outcome or product of the practice, process, or activity?” and may derive from previous implementation metrics. • *Impact metrics* answer the question, “What mission-related benefits (or costs) are associated with the practice, process, or activity?” and need to consider specific organizationally defined parameters beyond cyber security, such as budget and resource constraints.
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 an input into the formula for calculating the metric.
Target	Threshold for a satisfactory rating for the measure, such as milestone completion or a statistical measure. 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.
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.

Table B-1 (continued)
Metrics Development Template

Field	Data
Responsible Parties	Indicate the following key stakeholders: • Information Owner: Identify organizational component and individual who owns required pieces of information; • Information Collector: Identify the organizational component and individual 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 individual who will receive the data.
Data Source	Location of the data to be used 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 offers a sample of actionable metrics that utilities may leverage for the creation of a security metrics program. It is based on a collection of existing guidance, research initiatives, and outreach with utilities and external organizations. Most notably, the example metrics combined the template for 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 Cybersecurity Framework, as well as the DOE Cybersecurity Capability Maturity Model. While each organization will need to tailor these to their own risk management purposes, the foundational elements should aid utilities in their decision making process to adopt new metrics. These are not intended for adoption as a complete set of metrics, nor are they intended to meet regulatory requirements. Rather, the examples are designed to highlight various uses for metrics in any security program, regardless of size or capabilities.

Many of the associated templates are followed by complementary metrics, which may be discussed in other technical updates.

Table B-2
Example metric 1: Incidents Requiring Manual Cleanup

Field	Data
Metric ID	**Incident Response 1**
Goal	Demonstrate the relative level of manual effort required to cleanup systems after virus detection.
Supporting C2M2 & NIST CSF 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)
Measurement	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
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 • 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 B-3
Example metric 2: Mean-Time-to-Fix (MTTF)

Field	Data
Metric ID	**Incident Response 2**
Goal	Measure the effectiveness of an organization or business unit to recover from incidents.
Supporting C2M2 & NIST CSF 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)
Measurement	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 B-4
Example metric 3: Cyber Security Workforce Management

Field	Data
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 C2M2 & NIST CSF Objectives	NIST CSF Category: Asset Management (ID.AM-6) C2M2 Objective: Assign Cybersecurity Responsibilities (WM-1)
Measurement	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 B-5
Example metric 4: Mean Cost to Mitigate Vulnerabilities

Field	Data
Metric ID	**Vulnerability Management 1**
Goal	Understand the relative level of effort required to mitigate vulnerabilities across different business units and facilities
Supporting C2M2 & NIST CSF Objectives	NIST CSF Category: Analysis (RS.AN) and Mitigation (RS.MI) C2M2 Objective: Reduce Cybersecurity Vulnerabilities (TVM-2)
Measurement	Average (mean) $USD to 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 to Mitigate Vulnerabilities ($)

Table B-6
Example metric 5: Percent of Changes with Security Review

Field	Data
Metric ID	**Change Management 1**
Goal	Demonstrate the level of security considered for all change and configuration management practices across the organization
Supporting C2M2 & NIST CSF Objectives	NIST CSF Category: Information Protection Processes and Procedures (PR.IP) C2M2 Objective: Manage Changes to Assets (ACM-3)
Measurement	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.

C
ADDITIONAL METRICS FOR FURTHER INVESTIGATION

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. The table below highlights proven metrics from other industries that could be applied in the utility environment, though further research and piloting may be required. EPRI plans to continue research into security metrics for our industry.

Table C-1
Metrics for further investigation

Metric Description	Goal	NIST CSF Category	C2M2 Objective
Number of outgoing viruses caught at gateway	Indicate the rate of internal infections within an organization.	DE.AE	TVM-2
Mean Time to Incident Discovery	Track and improve the time it takes to detect a security incident.	DE.AE	IR-1
Number of cyber security skills mastered per employee	Track the status of employee training and resource adequacy across skillsets for cyber security in an organization.	ID.AM	WM-1
Mean Time between Security Incidents	Much like the operations tracking of Mean Time between Failure, indicates the amount of activity within a particular environment.	DE.DP, RS.AN	IR-1, IR-3
Cost of Incidents	Track and decrease the total cost of incidents, from direct losses to cost of recovery, over time. Can also be tracked as a mean or average cost.	RS.AN	IR-3

Table C-1 (continued)
Metrics for further investigation

Metric Description	Goal	NIST CSF Category	C2M2 Objective
Percentage of Systems without Known Severe Vulnerabilities	A basic vulnerability management metric for reporting what systems have severe (CVSS base score > 7.0)[1] vulnerabilities. Tracking should be different for OT and IT systems.	DE.AE	TVM-2
Mean Time to Patch	Track and improve the time it takes to patch across both IT and OT environments.	PR.IP	ACM-3, TVM-2
Percentage of Changes with Security Exceptions	Track and decrease the total number of system changes that receive security exceptions, with the goal of decreasing complexity and management of those systems. Must be tracked separately across OT and IT.	ID.RA	RM-1
Percentage of Applications Subject to Risk Assessment	Indicate a relatively mature risk management process by assessing applications in both OT and IT environments, with the goal of trending this measurement upwards over time.	ID.RA	RM-1
Information Security Budget Allocation	Separate and track each security activity (i.e., change and configuration management, vulnerability management, identity and access management, etc.) as percentages of the total budget.		CPM-2

[1] Common Vulnerability Scoring System (CVSS) is an open industry standard for assessing the severity of cyber security vulnerabilities. It calculates a base score based on a function of impact and exploitability and is used to prioritize mitigation plans and response.

Table C-1 (continued)
Metrics for further investigation

Metric Description	Goal	NIST CSF Category	C2M2 Objective
Compliance or Coverage of Information Security Practices	This metric can be separated into multiple categories (as needed by the organization), mirroring the budget allocation. Compared to total number of systems or assets, measure the amount that need to comply with standards or are covered by other information security practices across OT and IT.		CPM-1, CPM-2

The Electric Power Research Institute, Inc. (EPRI, www.epri.com) conducts research and development relating to the generation, delivery and use of electricity for the benefit of the public. An independent, nonprofit organization, EPRI brings together its scientists and engineers as well as experts from academia and industry to help address challenges in electricity, including reliability, efficiency, affordability, health, safety and the environment. EPRI also provides technology, policy and economic analyses to drive long-range research and development planning, and supports research in emerging technologies. EPRI's members represent approximately 90 percent of the electricity generated and delivered in the United States, and international participation extends to more than 30 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

© 2015 Electric Power Research Institute (EPRI), Inc. All rights reserved. Electric Power Research Institute, EPRI, and TOGETHER…SHAPING THE FUTURE OF ELECTRICITY are registered service marks of the Electric Power Research Institute, Inc.

3002005947

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