The Center for Internet Security

The CIS Security Metrics

November 1st

2010

Organizations struggle to make cost-effective security investment decisions; information security professionals lack widely accepted and unambiguous metrics for decision support. CIS has established a consensus team of industry experts to address this need. The result is a set of standard metric and data definitions that can be used across organizations to collect and analyze data on security process performance and outcomes.

This document is a guide to help organizations get metrics programs started quickly and effectively, using the CIS Security Metrics Definitions.

CIS Security Metrics – Quick Start Guide v1.0.0

Contents

Terms of Use Agreement

The nonprofit Center for Internet Security ("**CIS**") provides consensus-oriented information security products, services, tools, metrics, suggestions, and recommendations (the "**CIS Products**") as a public service to Internet users worldwide. **Downloading or using any CIS Product in any way signifies and confirms your acceptance of and your binding agreement to these CIS Terms of Use**.

CIS Terms of Use

Both CIS Members and non-Members may:

- Download, install, and use each of the CIS Products on a single computer, and/or
- Print one or more copies of any CIS Product that is in a .txt, .pdf, .doc, .mcw, or .rtf format, but only if each such copy is printed in its entirety and is kept intact, including without limitation the text of these CIS Terms of Use.

Under the Following Terms and Conditions:

- **CIS Products Provided As Is.** CIS is providing the CIS Products "as is" and "as available" without: (1) any representations, warranties, or covenants of any kind whatsoever (including the absence of any warranty regarding: (a) the effect or lack of effect of any CIS Product on the operation or the security of any network, system, software, hardware, or any component of any of them, and (b) the accuracy, utility, reliability, timeliness, or completeness of any CIS Product); or (2) the responsibility to make or notify you of any corrections, updates, upgrades, or fixes.
- **Intellectual Property and Rights Reserved**. You are not acquiring any title or ownership rights in or to any CIS Product, and full title and all ownership rights to the CIS Products remain the exclusive property of CIS. All rights to the CIS Products not expressly granted in these Terms of Use are hereby reserved.
- **Restrictions.** You acknowledge and agree that you may not: (1) decompile, dis-assemble, alter, reverse engineer, or otherwise attempt to derive the source code for any software CIS Product that is not already in the form of source code; (2) distribute, redistribute, sell, rent, lease, sublicense or otherwise transfer or exploit any rights to any CIS Product in any way or for any purpose; (3) post any CIS Product on any website, bulletin board, ftp server, newsgroup, or other similar mechanism or device; (4) remove from or alter these CIS Terms of Use on any CIS Product; (5) remove or alter any proprietary notices on any CIS Product; (6) use any CIS Product or any component of a CIS Product with any derivative works based directly on a CIS Product or any component of a CIS Product; (7) use any CIS Product or any component of a CIS Product with other products or applications that are directly and specifically dependent on such CIS Product or any component for any part of their functionality; (8) represent or claim a particular level of compliance or consistency with any CIS Product; or (9) facilitate or otherwise aid other individuals or entities in violating these CIS Terms of Use.
- **Your Responsibility to Evaluate Risks**. You acknowledge and agree that: (1) no network, system, device, hardware, software, or component can be made fully secure; (2) you have the sole responsibility to evaluate the risks and benefits of the CIS Products to your particular circumstances and requirements; and (3) CIS is not assuming any of the liabilities associated with your use of any or all of the CIS Products.
- **CIS Liability.** You acknowledge and agree that neither CIS nor any of its employees, officers, directors, agents or other service providers has or will have any liability to you whatsoever (whether based in contract, tort, strict liability or otherwise) for any direct, indirect, incidental, consequential, or special damages that arise out of or are connected in any way with your use of any CIS Product.
- **Indemnification.** You agree to indemnify, defend, and hold CIS and all of CIS's employees, officers, directors, agents and other service providers harmless from and against any liabilities, costs and expenses incurred by any of them in connection with your violation of these CIS Terms of Use.
- **Jurisdiction**. You acknowledge and agree that: (1) these CIS Terms of Use will be governed by and construed in accordance with the laws of the State of Maryland; (2) any action at law or in equity arising out of or relating to these CIS Terms of Use shall be filed only in the courts located in the State of Maryland; and (3) you hereby consent and submit to the personal jurisdiction of such courts for the purposes of litigating any such action.

Special Rules for CIS Member Organizations:

CIS reserves the right to create special rules for: (1) CIS Members; and (2) Non-Member organizations and individuals with which CIS has a written contractual relationship. CIS hereby grants to each CIS Member Organization in good standing the right to distribute the CIS Products within such Member's own organization, whether by manual or electronic means. Each such Member Organization acknowledges and agrees that the foregoing grants in this paragraph are subject to the terms of such Member's membership arrangement with CIS and may, therefore, be modified or terminated by CIS at any time.

Introduction

This guide was created to help organizations quickly implement and start metrics programs based on the CIS Security Metric Definitions. This guide has been designed to help organizations select what metrics to implement, create the data and metric results, and present them in an effective manner.

CIS Consensus Metrics

The CIS Consensus Metrics were created by volunteer and contract subject matter experts using a consensus process. Consensus participants provide perspective from a diverse set of backgrounds including consulting, software development, audit and compliance, security research, operations, government, and legal. The result is a set of twenty metric definitions covering several business functions, published as the CIS Security Metrics.

Steps to Create a Metrics Program

In order to create a metrics program, organizations need to follow these steps. Guidance on using the CIS metrics and the CIS Balanced Scorecard is provided for each step.

1. **Selecting Metrics**. A first set of metrics to be used must be chosen. The recommended initial set is those metrics used for the CIS Security Performance Scorecard. Additional or different metrics can be chosen depending on the organization's requirements.
2. **Creating Datasets**. Data sources for the metrics will be determined and the data needed for metrics collected. Dataset definitions are provided for all the Consensus Metrics.
3. **Implementing Metrics**. Metric Results will be calculated according to metric definitions.
4. **Presenting Results**. Metric results should be presented in a clear manner that assists in decision making. The CIS Security Performance Scorecard should be used to communicate monthly metric results to your organization.
5. **Growing a Metrics Program**. Once a metrics program is in place, additional metrics and dimensions can be added to increase the decision making capabilities.

Selecting Metrics

Organizations do not need to implement all of the CIS security metrics to implement a successful program . In fact, the best result comes from starting small: selecting those metrics and business functions that are of immediate interest to your organization.

Business Functions

CIS has defined twenty-eight significant metrics that cover seven business functions. The chart below provides an overview of these business functions and associated metrics. More metrics will be defined in the future for these and additional business functions.

Business Functions		
Function	**Management Perspective**	**Defined Metrics**
Incident Management	How well do we detect, accurately identify, handle, and recover from security incidents?	• Cost of Incidents • Mean Cost of Incidents • Mean Incident Recovery Cost • Mean-Time to Incident Discovery • Number of Incidents • Mean-Time Between Security Incidents • Mean-Time to Incident Recovery
Vulnerability Management	How well do we manage the exposure of the organization to vulnerabilities by identifying and mitigating known vulnerabilities?	• Vulnerability Scanning Coverage • Percent of Systems with No Known Severe Vulnerabilities • Mean-Time to Mitigate Vulnerabilities • Number of Known Vulnerabilities • Mean Cost to Mitigate Vulnerabilities
Patch Management	How well are we able to maintain the patch state of our systems?	• Patch Policy Compliance • Patch Management Coverage • Mean-Time to Patch • Mean Cost to Patch
Configuration Management	What is the configuration state of the systems in the organization?	• Percentage of Configuration Compliance • Configuration Management Coverage • Current Anti-Malware Compliance
Change Management	How do changes to system configurations affect the security of the organization?	• Mean-Time to Complete Changes • Percent of Changes with Security Reviews • Percent of Changes with Security Exceptions
Application Security	Can we rely on the security model of business applications to operate as intended?	• Number of Applications • Percent of Critical Applications • Risk Assessment Coverage • Security Testing Coverage
Financial Metrics	What is the level and purpose of spending on information security?	• IT Security Spending as Percent of IT Budget • IT Security Budget Allocation

Choosing Which Metrics to Implement

Setting goals for metrics

Select metrics to implement based on the needs and requirements of the organization. The production of metrics is not an end in itself; rather select metrics according the organization's goals for the metrics program. Choose metrics that can provide decision-support for questions ranging from "Is the impact of security incidents decreasing over time?" to "Should business practices be modified?" While there will be a high-level goal, such as "Improve management decision making around risk and security," it is important to drill down from a high-level to specific and actionable goals for the initial metric program.

The path to achieve specific tasks is to decompose higher-level goals by asking what answers would indicate that the goals were met. For example, "Do we currently have many systems in severely vulnerable states? Have we assessed the risk of our new applications?"

In many cases, particular areas of improvement may have already been identified and specific goals, such as "Deploy patches to meet defined service level agreements," can be set. Management may want to pursue a specific project, such as consolidating to a single vulnerability scanner. In this case, metrics could be used to measure vulnerability management performance before and after the project to determine its effectiveness.

Selecting from the CIS Metrics

Based on the business functions and metrics table, it is easy to see what metric definitions are currently available. Select one or more of the supporting metrics. While it is not necessary to select more than one metric per function, interpreting the results can be more effective when a small number of metrics that support each other are used together. For example, the percentage of systems complying with current patch policy is likely to increase if the total percentage of systems under the patch management system's coverage is made a priority.

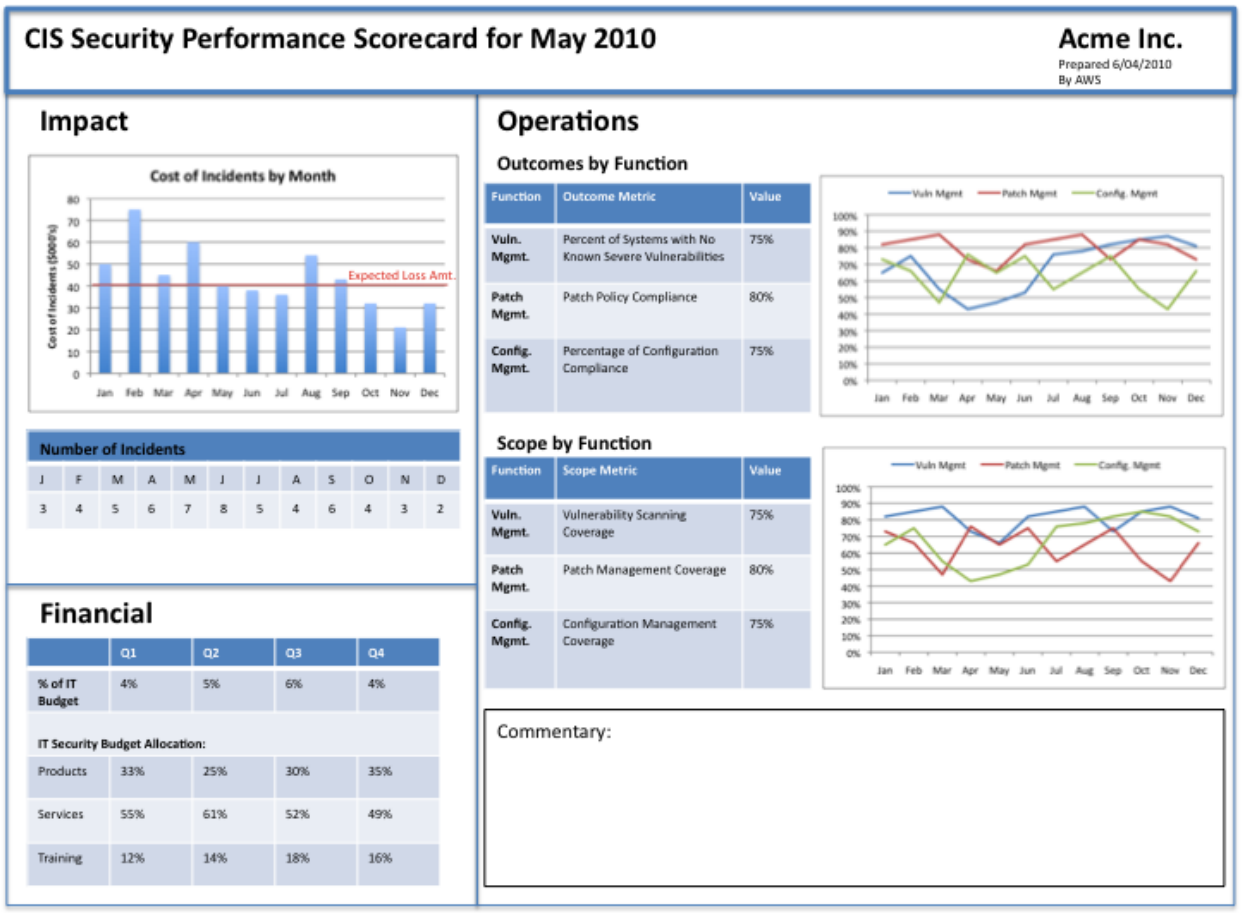
Metrics for the CIS Balance Scorecard

Organizations can quickly determine their choice of CIS metrics by implementing the CIS Balanced Security Scorecard. The following table lists the set of metrics needed for complete coverage of the CIS scorecard.

Scorecard Area	Action	Required Metrics
Impact	Report on security incidents and their impact on the organization.	1. Number of Incidents 2. Cost of Incidents
Performance by Function: Outcomes	Report the outcome of business functions' Configuration Management, Patch Management and Vulnerability Management.	3. Configuration Policy Compliance (using CIS benchmarks) 4. Patch Policy Compliance (using current patch level) 5. Percent of Systems with No Known Severe Vulnerabilities (using CVSS base scores)
Performance by Function: Scope	Report the scope of business functions and the scope of outcome metrics for those functions.	6. Configuration Management Coverage 7. Patch Management Coverage 8. Vulnerability Scanning Coverage
Financial Metrics	Report on the allocation and efficiency of security spending	9. IT Security Spending as Percent of IT Budget 10. IT Security Budget Allocation

The CIS Security Scorecard

The CIS scorecard was developed to provide an easy way to report monthly security metrics within your organization. This scorecard focuses on the impact of security incidents, as well as on tangible security activities in the organization.



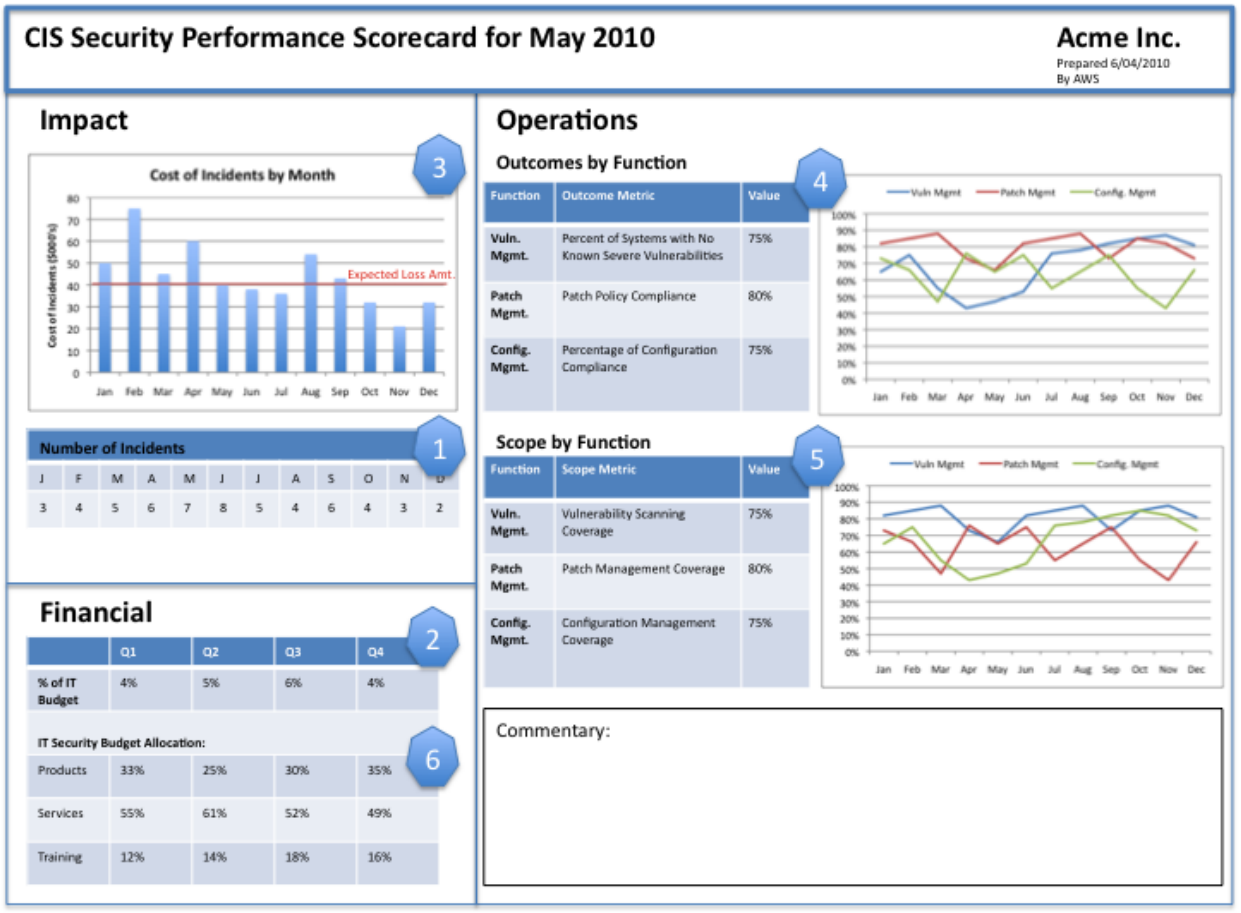
The output of operational activities is combined with security outcome information to present a clear picture of the state of an organization's information security program. Because this scorecard relies primarily on automated and sufficiently reliable data gathering, it can provide a reliable and repeatable method for reporting security performance while minimizing ambiguity.

The scorecard has three main sections:

1. **Impact** of security incidents on the organization
2. **Operations** of business functions, with both the key outcome indicator as well as a scope metric
3. **Financial** costs and allocations security operations

Implementing the CIS Security Scorecard

Implement the scorecard in stages, starting with the most important metrics and expanding into metrics that require more automation in data gathering and processing. With the complete scorecard as a goal, the recommended steps for implementation are shown below:



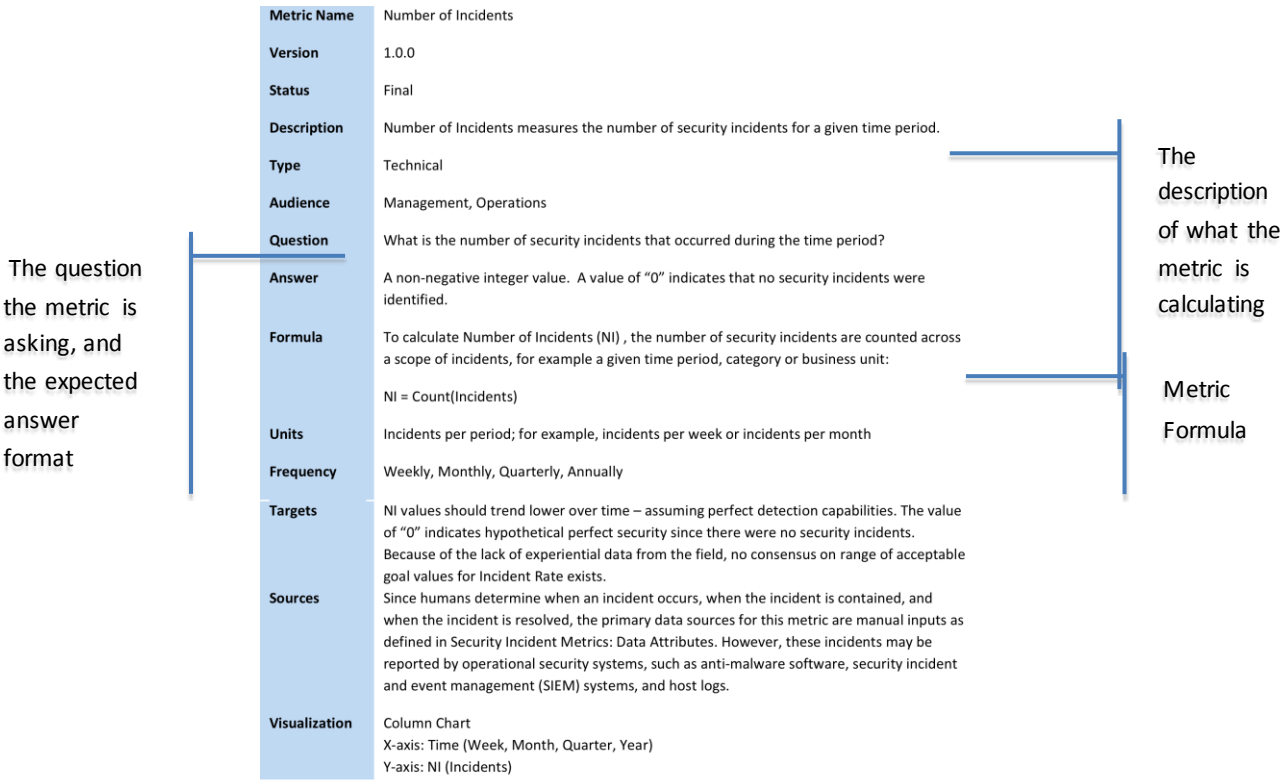
1. **Number of Incidents**. A foundational metric that provides a baseline as other metrics are implemented.
2. **IT Security Spending as Percent of IT Budget**. Provides a baseline to track overall security spending.
3. **Cost of Incidents**. Shows the impact of security incidents to the organization.
4. **Outcome metrics**. Provides key indicators of the outcome of the key functions. Data should be available from automated systems.
5. **Scope Metrics**. Shows the scope of the organization to which the outcome metric applies. Data comes from automated systems with inventory and exception lists.
6. **IT Security Budget Allocation**: Once tracking metrics are in place, changes to spending can be tracked against operational outcomes and impact on the organization.

Implementing Metrics

Using CIS Metric Definitions

Once you have selected the metrics you want to use, you can implement them following the definitions given in the CIS Security Metrics document. Here is an example of a simple metric definition:

The metric definition is composed of several elements, the most important being the formula, which defines how the metric result should be calculated. The data that is used to drive this metric is defined in the Data Set Definitions for each Business Function.

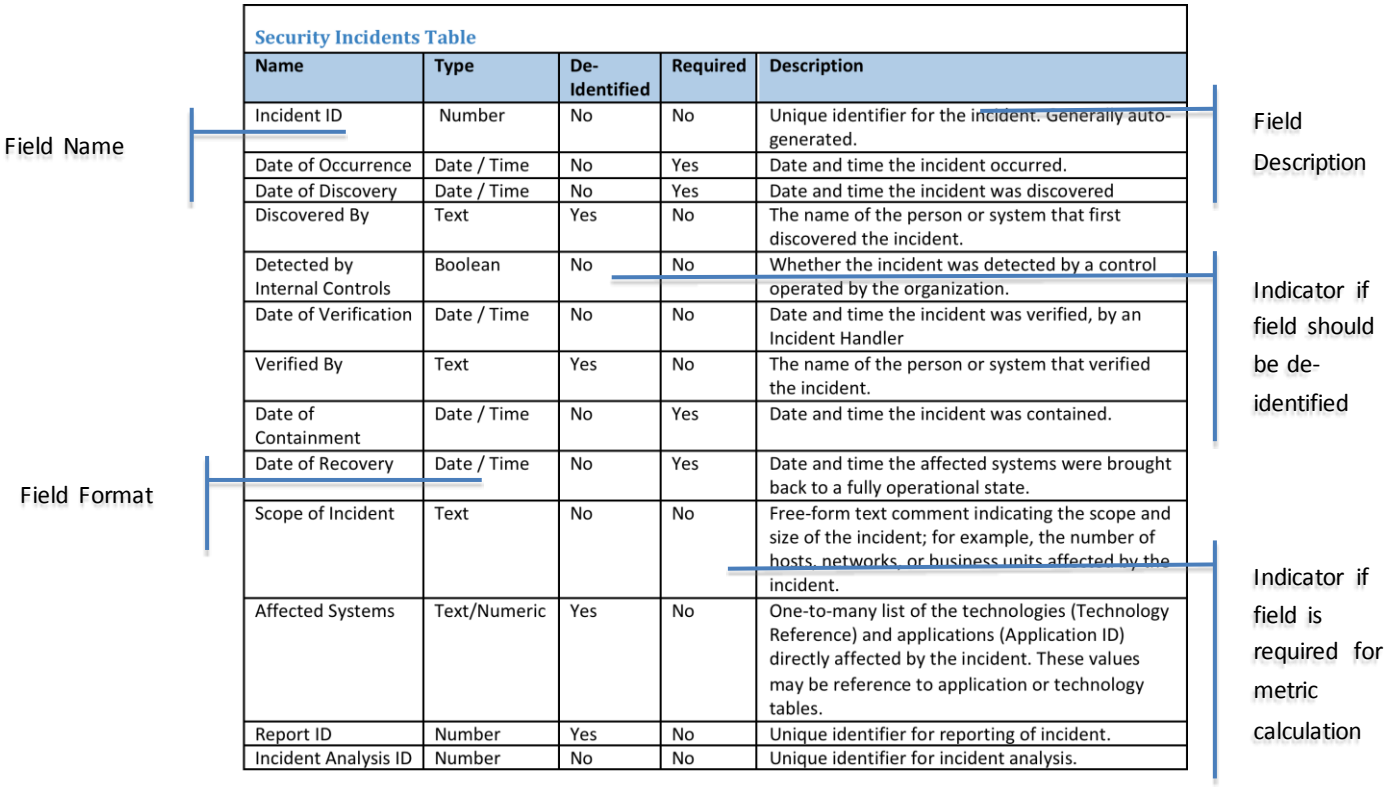


Data Set Definitions

The data required to drive metrics is provided in the dataset definitions. For example, the metric definition of the Number of Incidents uses the following datasets (also defined in CIS Security Metrics):

- **Security Incidents Table**. Contains information about each security incident in the organization.
- **Security Incident Classification Table**. Provides additional information about the incident including the type as well as priority, criticality, country of origin, etc.
- **Security Incident Impact Analysis Table**. Contains information from the incident analysis, such as the loss amount.
- **Security Incident Reporting Table**. Contains demographic information on the reporting organization.

Each dataset is defined in a table that shows each field, the type of data expected, whether or not that data could be used to identify the organization, if the field is required for metric calculation, and a description of the field.



Security Incidents Table

Name	Type	De-Identified	Required	Description
Incident ID	Number	No	No	Unique identifier for the incident. Generally auto-generated.
Date of Occurrence	Date / Time	No	Yes	Date and time the incident occurred.
Date of Discovery	Date / Time	No	Yes	Date and time the incident was discovered
Discovered By	Text	Yes	No	The name of the person or system that first discovered the incident.
Detected by Internal Controls	Boolean	No	No	Whether the incident was detected by a control operated by the organization.
Date of Verification	Date / Time	No	No	Date and time the incident was verified, by an Incident Handler
Verified By	Text	Yes	No	The name of the person or system that verified the incident.
Date of Containment	Date / Time	No	Yes	Date and time the incident was contained.
Date of Recovery	Date / Time	No	Yes	Date and time the affected systems were brought back to a fully operational state.
Scope of Incident	Text	No	No	Free-form text comment indicating the scope and size of the incident; for example, the number of hosts, networks, or business units affected by the incident.
Affected Systems	Text/Numeric	Yes	No	One-to-many list of the technologies (Technology Reference) and applications (Application ID) directly affected by the incident. These values may be reference to application or technology tables.
Report ID	Number	Yes	No	Unique identifier for reporting of incident.
Incident Analysis ID	Number	No	No	Unique identifier for incident analysis.

The source used to produce the data will depend on the specific products and systems in use in an organization. Common sources for this data are described in the definition. Some treatments may be necessary to match the data format, such as converting from network scan IP addresses to system names used as identifiers in the technologies table and that treatment may be used in order to identify system groups and owners.

Full schema definitions including xml formats are also available for use in automating the data collection process. See the CIS website (http://www.cisecurity.org) for more details.

Important items to note during the data collection phase are the following:

- Data may need to be aggregated from more than one system. There may be multiple instances of a product or system in an organization (e.g. for different divisions). This data should be combined for metric calculation, although you can add a column indicating the original source to provide additional dimensions to the data.
- It is important to understand the scope—what is and isn't included in the data. This will be important to the interpretation and use of the final metric results. For instance, production servers may not be included in network scanning activities.

Creating Datasets

The first step in calculating metric results is to create the datasets needed to drive the metrics calculations. Datasets are defined for each business function and are designed to be able to be generated by the systems and processes already in place in most organizations. While the scorecard provides a means for collecting and assessing a diversity of data, the required data fields are both limited and clearly marked. As the organization establishes its metrics program, the degree of data collections can be increased to widen the scope of metric results as well as provide more details for those results.

Creating the Data

The first step is to examine the datasets used by the metric being implemented. These datasets will indicate the required fields and any additional fields that may be of interest. Datasets also indicate where dimensions could be added to the data to provide more detailed information. With the data set definitions in hand,

1. Identify the systems in the organization that are possible data sources. Generally these are the products and systems directly related to the business function (such as network scanners) and any asset management systems. There are three broad classes of data sources:

    a. Sources of information related to the security activities. Generally these are the security products themselves, such as network scanners, patch management systems, etc.

    b. Sources of information related to security issues such as vulnerability and patch information. This information may be included in some security systems or could be in-house or in online databases, such as the National Vulnerability Database

    c. Sources of information related to the systems and technologies in the organization, such as asset management systems. The primary challenge for security metrics is mapping data from security systems to asset management systems. In some cases, much of this information will also be included or derived from the security product or systems.

2. Based on the metric definition, identify the data sources for each field in the metric's dataset and extract the relevant data. This data can come directly from existing databases or extracted reports. Be sure to extract data from each source that matches the appropriate time period for the metric. Data Cleanup may be necessary. Check for format issues, such as date/time values and the handling of null fields.

    > ***Example*****:** *For the Identified Vulnerabilities Dataset, identifying the data sources could consist of aggregating all the scan results to cover the entire organization, by combining subnet scans that occur over the course of one week each month, being sure to remove overlapping data, and using an extract from the asset management system taken at the end of the month.*

3. Field names and formats should be mapped to meet the dataset standard. This will ensure that standard metrics can always be applied to the datasets. De-identification can also occur at this time, if the metric data is to be shared with others. De-identification is the process of removing or anonymizing information that could be used to identify the submitting organization. De-identification enables sharing source data for benchmarking or other purposes while preserving the privacy of the submitters.

Dimensions

What are Dimensions

Dimensions are a way of providing additional detail to metric results for specific subsets of systems (such as "servers") or states (such as "critical patches"). This can be done when you have added additional tags & classifications to the source datasets, such as the business unit that owns the system, or the business applications it supports. For the dataset example above, the following fields could be added to this with organization-specific data for each identified vulnerability or system:

- Detect by External Scan (i.e. from the Internet outside the organization)
- By Network Location scanned (i.e. subnets that represent different datacenters)

With dimensional data, it is possible to view metric results for specific categories of systems and types of activities and vulnerabilities, such as "severe vulnerabilities on all servers being used for customer-facing web applications." Dimensional information is often very business specific, tying metric results to the specific organization, purpose of systems, and business activities.

To continue the example, by enhancing the dataset with additional organization-specific data, it could be possible to present metric results for a metric such as the Percentage of Systems with Known Severe Vulnerabilities with dimensions such as:

- Percentage of Systems with Known Severe Vulnerabilities **that are Internet-Facing**
- Percentage of Systems with Known Severe Vulnerabilities **by Location**

Creating dimensional data

Adding dimensions to data can significantly increase the value and uses of security metrics in an organization. Creating dimensional data varies depending on the systems and source locations in an organization. Some types of dimensional data such as patch criticality or vulnerability severity are often included in the primary data sources and can be easily included in a dataset. These two examples are common enough to be part of the required dataset.

Other types of dimensions, such as which business unit or division owns a particular system or the location of the system, are not always included in the primary sources. In addition to finding primary sources for metric data, primary sources for dimensional data should be identified. These sources can include asset management systems for data such as technology owners, the value of business applications, physical locations, etc. In other cases dimensional data is encoded in other sources, such as the nomenclature of system names or usernames.

Some dimensional data, such as application values may only exist in spreadsheets or lists. Generally in these cases it is necessary to find additional sources of this dimensional data and join them to the metric dataset on a key such as the IP address or System Name. How this process occurs will need to be determined on a case-by-case basis. For example, vulnerability scanning results may identify systems by IP addresses, while technologies may be tracked by system names. There are solutions, such as reverse DNS lookups to match these results. As possible dimensions are identified, the value of creating sources where none already exist can be assessed.

Dimensional data is most valuable when presented in the same units as the metric result (i.e. at a per-host or per-vulnerability level) so that the organization can calculate metric results for that dimension.

Identified Vulnerabilities Table

Name	Type	De-identified	Required	Description
Reference ID	Number	No	Yes	Unique identifier for the vulnerability instance. Generally auto-generated
Vulnerability Reference ID	Number	No	Yes	Reference to the Vulnerability in the Vulnerability Information Table
			. . .	
Scan Type	**Text**	**No**	**No**	**"Internal" for scans from within the internet network, or "External" for Internet-based scans**
Location	**Text**	**Yes**	**No**	**Mapping from subnet to text label of location, ex: 192.1.x.x = Headquarters, 192.2.x.x = =Datacenter, 192.3.x.x = Manufacturing, 192.4.x.x = Research**

Dimension fields added to Dataset

Organization -specific mappings

This standardization will require additional calculations, as the metric results should be produced for the entire dataset, as well as for each dimensional grouping. Metric results are calculated the same way, either for the entire dataset or for each set of intersecting dimensions, grouped by each value in a dimensional field, such as by location, severity, or priority. Fortunately, when metric calculations are automated, this is a relatively easy task.

Creating Metric Results

Once metric datasets are ready, it is possible to calculate metric results. Based on the formula provided in the metric definition, metrics should be calculated.

1. Use the formula for the metric provided in the metric definitions.
2. Scope and filter the metric dataset for the specific metric and time period being calculated.
3. Calculate results for the metric. Ideally this can be done automatically instead of manually to facilitate regular metric calculations. Calculate metric results for each dimension of interest, including intersections of key dimensions, such as "Severe Vulnerabilities on Internet-Facing Systems."
4. Store metrics results. Ideally this is in a form that makes it possible to easily access the results for time-series calculations and metric visualizations but that also stores information in a read-only and un-modifiable format to preserve the results. While possible, it is not necessary to store all the source data used to calculate metric results. It is the results that are of primary interest, and the storage of significant datasets can cause unnecessary complications.

Presenting Metrics

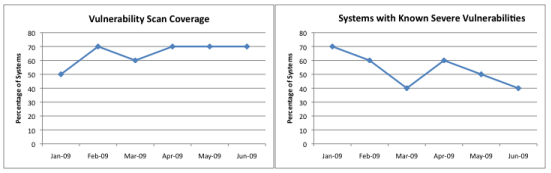
There are many ways that metrics results can be presented. There is a tendency to report everything possible. Instead, report on a limited set of metrics that support existing decision-making processes where corrective action can occur on a regular basis.

When creating charts and tables of metric results, it is important to keep metric results clear and not introduce 'chart-junk'. Keeping metric results clear will produce clean, simple charts and tables that are easy to understand. Metric results do not all have to be presented as charts, or even in the same way.

There are several available sources for guidance on presenting metrics. These sources suggest best practices for visual organization, formatting, and choosing audiences for metrics (see **Resources**). The CIS Consensus Metrics are designed to be presented in conjunction with the CIS Security Scorecard. This is a set of outcome-focused metrics that can be used to consistently communicate the state of security results and performance for information security business functions, enabling managers to see areas that may be in need of focus and resources, and to show progress over time resulting from the application of resources or process changes.

Using Additional Metrics

Additional scorecards may be presented to the more technical audiences to provide greater context to metrics; for instance, it is useful to present a metric result for the percentage of systems with known severe vulnerabilities as a key indicator. However, those tasked with ownership of that metric result will need more data to manage the process. If the scope of vulnerability scanning is not well understood and consistent, it will also be necessary to present metric results for the vulnerability scanning coverage as well. In this way, the audience can understand what portion of the organization was scanned in addition to what was found and take appropriate action.



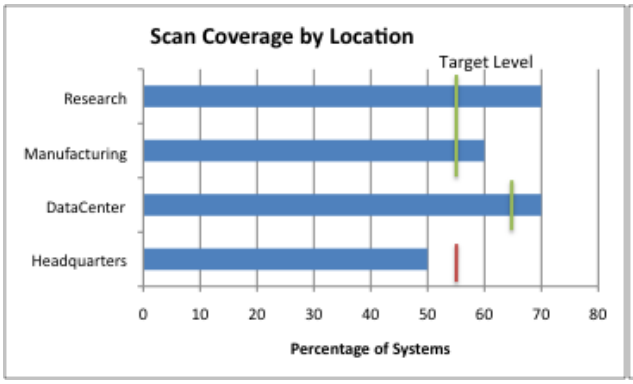
Meaning and Guidance

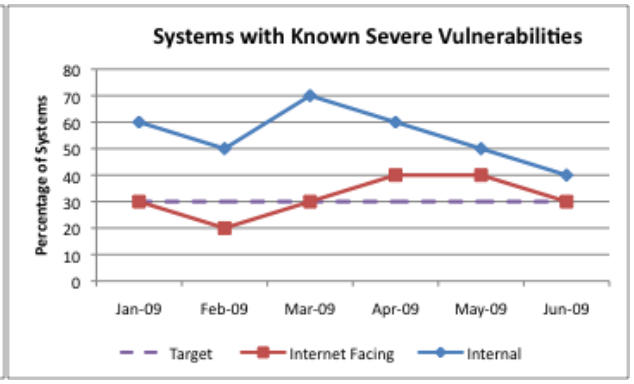
It is important to provide annotation (for example, to link a discontinuity in data with a specific event) as well as guidance and interpretation of the results. The security people are the experts – they should summarize the results and provide the metric results. Metrics should be used as supporting data to enhance the organization's understanding of security and provide interpretations that are supported by evidence. In all cases, the limitations of metrics need to be considered when interpreting the results. Metrics can provide valuable data points but do not blindly "answer" security problems. For example, vulnerability metrics only report those vulnerabilities that are detectable and were checked for on a subset of the organization's systems. There is still a set of unknown and undetectable vulnerabilities that may be present. Despite these limitations, this may be the best data available with which to manage the vulnerability state of the organization.

Mapping Metrics to the Business

Dimensions allow metrics results to be directly mapped to the business, showing results for specific subsets of systems, such as risk assessments on critical applications. Metrics can also be used to provide additional details about the scope and different aspects of security process performance or to track the progress of security initiatives.

The combination of dimensions makes it possible to identify and highlight concentrations of risk, such as severe vulnerabilities on servers used by the consumer-facing division. While some concerns may be universal, others may be firm specific. This type of specificity makes it possible to get metrics results that are very specific to the needs and risks of the organization's business operations. For example, consider the same metrics used in the prior example, now enhanced with firm-specific dimensions:





The use of dimensions in metric results can be very powerful for identifying areas that require management attention and resources and for driving change in the organization.

Dimensions also allow metrics results that are directly relevant to the audience to be presented. For example, managers whose line of business relies on Internet-facing web-servers could view metrics results for only the set of systems their business relies upon, instead of seeing results that lump all systems together and that will have limited meaning. The names used for groups of systems or people or locations and the order in which divisions are presented should match the way other metrics and operating results are presented in the organization. This guideline makes it easier to understand the affected group and correlate security performance with other activities and reports.

Using metrics in your organization

In order to get a metrics program started, it is best to start small, with one business function or one system. As people become familiar with security metrics and see them in regular production, it will be easier to expand the program into new areas and more metrics. Generally, once metric production begins, there is a flood of requests for additional metrics. This demand can initiate any support needed for personnel or technical assistance. To get started rapidly, there are several steps that should be taken to make effective use of metrics:

1. Identify a metrics team. Who will own this metrics project? The team should consist of at least one person who is familiar with the technical systems that can provide data as well as extract, and process data (and reduce reliance on outside groups). An ideal team would also include someone that is familiar with or can research how business managers could use metric results.

2. Pick a specific audience to support with metrics. This will limit the number of metrics you have to implement initially. It is best to choose an audience that has control over the systems that will be used to produce the metrics.

3. Pick a metrics area that is relevant, easy to access, and has data. Start with metrics that are easier to produce rather than ones that may challenge systems and sources. The metrics should be relevant to the audience and their short- or medium-term goals (such as process improvement or their next reporting cycle) to provide a material impact.

4. Identify metrics and data sources. Find and extract the data necessary to create metrics. Dimensions should be identified so that next steps and future improvements can be discussed. If it is easy to add additional details and business context to metrics, they can be implemented, but don't try to do too much initially and become mired in the technical project of connecting systems together.

5. Create an example of the metrics and format and get stakeholder approval. In order to be effective, the audience for metrics needs to be in agreement with what metrics will be collected and how they will be presented.

6. Implement metrics. Ideally metrics calculation will be automated to facilitate regularly repeated collection. There are several ways this can be done, from dedicated metrics products to BI tools, to scripts and stored procedures. Store metrics results in a retrievable but archived format. The results should be easy to access, reference, and incorporate past metric results in a read-only format. It may be burdensome to store all the source data that was used to calculate metric results. The primary value is in the final results themselves.

7. Include a process for metrics review and modification. Review metrics on a regular basis to determine if they are still relevant, require modification, or if new metrics should be created. For example, an organization could review metrics annually, and new metrics created to track performance toward each year's goals.

Enhancing the metrics program

Once the metrics program is underway, there will be opportunities to enhance and expand the program. Once metrics are being used regularly, support will be present for an additional investment. There are three ways the metrics program can be expanded:

- Additional metrics can be added in the same business function area. As part of managing a metrics program there should be a process to regularly review existing metrics and suggest additional metrics. Metrics that are designed to drive changes in behavior should be replaced when goals are met and new goals arise (for example, bringing systems under patch management, and then reducing the mean-time to patch). Add additional metrics in sets for different audiences (for example, more process for operations management), more dimensions for business reasons, etc.
- Metrics for new business functions can be added. New projects and business goals can lead to new sets of metrics in additional business functions.
- Dimensions providing more detailed metrics can be added to existing metric sets. Standard metrics can continue to be used with additional enhanced metrics directly addressing specific groups such as “for production servers," or “by customer.”

References

There are several additional resources for metrics, ranging from books on the topic to papers and websites:

- The CIS Security Metrics, http://www.cisecurity.org
- securitymetrics.org website at http://www.securitymetrics.org
- Metricon Conference, information available at http://www.securitymetrics.org
- Chew, Swanson, Stine, Bartol, Brown, and Robinson. Special Publication 800-55: Performance Measurement Guide for Information Security (Rev 1). US National Institute of Standards and Technology, 2008
- Jacquith, Andrew, Security Metrics: Replacing Fear, Uncertainty, and Doubt, Addison-Wesley Professional, 2007
- Payne, Shirley C., A Guide to Security Metrics, SANS Institute, 2006