Persuading Senior Management

with Effective, Evaluated Security Metrics.

Peter Ohlhausen, President, Ohlhausen Research, Inc., Principal Investigator
Megan Poore, MS, Research and Workforce Analyst, GSX, Senior Analyst
Daniel McGarvey, Director, Security Programs, GSX, Subject Matter Expert
Lance Anderson, PhD, Workforce Solutions Practice Director, GSX, Technical Advisor

ASIS
FOUNDATION ™

Persuading Senior Management with Effective, Evaluated Security Metrics

Peter Ohlhausen, President, Ohlhausen Research, Inc., Principal Investigator

Megan Poore, MS, Research and Workforce Analyst, GSX, Senior Analyst

Daniel McGarvey, Director, Security Programs, GSX, Subject Matter Expert

Lance Anderson, PhD, Workforce Solutions Practice Director, GSX, Technical Advisor

2014

ASIS FOUNDATION™

Research funded by a grant from the ASIS Foundation

ii   EFFECTIVE, EVALUATED SECURITY METRICS—© ASIS Foundation 2014

About the Foundation

The ASIS Foundation is a 501(c)(3) nonprofit organization dedicated to fostering research and education opportunities that enhance the security profession.

The topics researched by the Foundation produce valuable and actionable knowledge for the security professional. Additionally, through the awarding of scholarships, the Foundation ensures that those pursuing a career in the field of security management are able to realize the highest academic achievements.

Foundation programs are supported solely by contributions from individuals, ASIS chapters, and other organizations that share its vision of advancing both the security profession and the professional.

https://foundation.asisonline.org

Principal Investigator: Peter Ohlhausen, President, Ohlhausen Research, Inc.

www.ohlhausen.com

Senior Analyst: Megan Poore, MS, Research and Workforce Analyst, GSX

Subject Matter Expert: Daniel McGarvey, Director, Security Programs, GSX

Technical Advisor: Lance Anderson, PhD, Workforce Solutions Practice Director, GSX

www.gskillsxchange.com

Acknowledgments

Contents

Executive Summary

Security metrics support the value proposition of an organization's security operation. Without compelling metrics, security professionals and their budgets continue largely on the intuition of company leadership. With metrics, the security function grounds itself on measurable results that correlate with investment, and the security professional can speak to leadership in a familiar business language. Security metrics are vital, but in the field and in the literature one finds few tested metrics and little guidance on using metrics effectively to inform and persuade senior management.

To address the gap, in spring 2013 the ASIS Foundation sponsored a major research project designed to add to the body of knowledge about security metrics and to empower security professionals to better assess and present metrics. The Foundation awarded a grant to Global Skills X-change (GSX), partnered with Ohlhausen Research, to carry out the project.

This report provides the project's findings, including its three practical, actionable products:

- The Security Metrics Evaluation Tool (Security MET), which security professionals can self-administer to develop, evaluate, and improve security metrics

- A library of metric descriptions, each evaluated according to the Security MET criteria

- Guidelines for effective use of security metrics to inform and persuade senior management, with an emphasis on organizational risk and return on investment

A. Methodology

With input from an advisory board and expert panel, the research team performed the following tasks:

- **Review and summarize literature on the use of security metrics to inform and persuade corporate management.** The review cites approximately 100 sources.

- **Develop and refine a Security Metrics Evaluation Tool (Security MET).** The Security MET is a written tool that security managers can use to assess the quality of specific security metrics. The tool was revised throughout the research process, based on feedback from the advisory board and expert panel.

- **Collect data to identify and evaluate current practices in the use of security metrics.** This task included an online survey and detailed follow-up interviews by telephone.

- **Create a database of evaluated security metrics.** The project report contains 16 metric summaries (Appendix B), each evaluated by three reviewers using the Security MET.

- **Develop guidelines for effective use of security metrics to persuade senior management.** Chapter VII of this report presents guidelines gathered from a variety of sources: the literature review, the online survey, the follow-up telephone interviews, the advisory board, and the expert panel.

B. Literature Review

The literature review examined reasons to use metrics, characteristics of existing metrics, methods for communicating metrics, and means of evaluating metrics. Overall findings from the literature:

- Descriptions of existing security metrics are often vague, making it difficult to adopt those metrics. The focus is more on counting events than creating meaningful, risk-based metrics.

- Strategies for communicating metrics are general and may be hard to implement.

- Typically, evaluation criteria are only presented at a conceptual level within the security literature, without explicit definitions.

- Few examples of empirically sound metrics (with statistical justification and evidence) are present within the security literature. Physical security and information security appear to have more metrics in use than other security fields.

C. Security Metrics Evaluation Tool

The Security Metrics Evaluation Tool (Security MET) is a written tool that security managers can use to assess the quality of specific security metrics. Users will be able to determine whether an existing or proposed metric possesses scientific validity, organizational relevance (such as clear alignment with corporate risks or goals), return on investment, and practicality. Basically, the tool was designed to help a user identify a metric's strengths and weaknesses so that the weaknesses can be corrected. The Security MET is presented in Appendix A.

The tool was developed through a lengthy, iterative process that involved synthesizing scientific literature, security industry standards, and input from metrics experts on the project's advisory board and expert panel. (The advisory board and expert panel consisted primarily of senior security professionals with experience in the use of security metrics.) To develop the criteria (the characteristics that make an empirically sound security metric), the research team turned to measurement and testing literature, as well as industry benchmarks, and developed criteria in three categories: technical, operational, and strategic.

The tool includes the following criteria for evaluating a security metric. Definitions for and relevant research associated with the criteria are presented in Section IV.

Technical Criteria – Category 1

1. Reliability
2. Validity
3. Generalizability

Operational (Security) Criteria – Category 2

4. Cost
5. Timeliness
6. Manipulation

<u>**Strategic (Corporate) Criteria – Category 3**</u>

    7. Return on Investment

    8. Organizational Relevance

    9. Communication

For each criterion, the Security MET presents a definition, concept illustration, behavioral summary scale, and sample applications to help users understand how to evaluate the metric. A score sheet is presented at the end of the Security MET to tabulate the metric's score across the nine criteria. Lower scores on particular criteria show where a metric has room for improvement.

The Security MET is designed to help the user review and understand all the behaviors associated with the criteria at varying levels. It establishes a common frame of reference for metrics users to employ when examining and rating their metrics. This frame of reference is further reinforced by the examples presented that highlight how the example metrics should be scored based on the criteria presented. Finally, this instrument is easy to score, imposes little to no time burden on staff, and could easily be placed on a wide variety of online systems.

D. Online Survey

On August 7, 2013, with the help of ASIS International and in concert with the ASIS Leadership & Management Practices Council, the research team invited more than 3,000 ASIS members to participate in an online survey. Invitations were e-mailed to all ASIS council members and the CSO Roundtable, plus an ASIS-created pool of top-level security professionals. A total of 297 people responded. Complete survey results, including detailed, open-ended responses, are presented in Appendix D.

Given the limitations of the sample (e.g., participation was optional, and those who chose to participate probably are not representative of all security managers), the survey did not attempt to ascertain the prevalence of particular metrics practices in the field. Instead, the survey helped the research team discover metrics practices and identify metrics users for follow-up interviews.

Survey Questions

Q1: Collection and Use of Security Metrics
Q2: Metric Comparison to External Benchmarks
Q3: Would You Use Metrics?
Q4: Measured Security Program Aspects
Q5: Who Records Metrics?
Q6: Metrics Provisions to Non-Security Persons
Q7: Metrics Provisions to Non-Security Persons
    – If No, Why Not?
Q8: Metrics Provisions to Non-Security Persons
    – Who?
Q9: Metrics Provisions to Non-Security Persons
    – How Often?
Q10: Metric Elements Shared with
    C-Suite Personnel

Q11: Most Important Metrics
    – Senior Management
Q12: Most Important Metrics – Why?
Q13: Metric Alignment With Risk/Objectives
Q14: Metric Alignment With Risk/Objectives
    – How?
Q15: Dashboard Tool Usage
Q16: Who Developed Dashboard Tool?
Q17: Third-Party Dashboard Tool Name
Q18: Metrics Interview Volunteers
Q19: Work Region
Q20: Desire Information Regarding Metrics

Respondents demonstrated a high degree of interest in the topic of metrics:

- Seventy-seven percent of respondents said they are collecting and using security metrics.

- Of respondents who said they are not using security metrics, 78 percent said they would use metrics if they knew more about how to create them and use them effectively.

- Out of all respondents, 55 percent said they would like to receive more information from ASIS regarding metrics and supplied their names and e-mail addresses.

They also provided the research team with a detailed view of the many ways in which security professionals are using metrics today:

- **Metrics topics.** Respondents were asked which aspects of the security program they measure. They were given a list of 13 categories (plus "other") and asked to check all that apply. The top five categories of metric focus were security incidents, criminal incidents and investigations, cost against budget, security training and education, and guarding performance (turnover, inspections, etc.).

- **Sharing and reporting.** Eighty percent provide their metric findings to persons outside the security department. Recipients of the information include senior management (listed by 79 percent of those who share metrics outside the security department), managers of other departments (59 percent), supervisors (51 percent), and people who report to the security department (47 percent). Those who share metrics provide the information quarterly (43 percent), monthly (40 percent), or annually (17 percent).

- **Topics shared with C-suite.** Respondents who share metrics with C-suite personnel were given a list of 13 categories of topics (plus "other") and asked which elements they share (selecting all that apply). The top choices were security incidents (80 percent), cost against budget (62 percent), criminal incidents and investigations (57 percent), regulatory compliance (44 percent), and risk analysis process (40 percent).

- **Alignment with organizational risk or objectives.** Eighty percent of respondents who use metrics said their metrics are tied to, aligned with, or part of the larger organizational risk process or organizational objectives.

- **Dashboard tool.** Only 44 percent of respondents using metrics perform their data collection, review, or sharing via a security management dashboard tool.

E. Metrics Summaries

The researchers developed 16 summaries of metrics that were in use in the security field as of 2013. The summaries were developed primarily through telephone interviews. Participants were identified through the project's online survey, which asked respondents if they were currently using metrics and would be willing to describe their practices to a researcher. About half the interviewees also supplied examples of the graphics they use to convey their metrics to senior management. All 16 summaries are presented in Appendix B, along with evaluations. Each metric was scored against the Security Metrics Evaluation Tool (Security MET) by two members of the project's expert panel and one member of the research team.

The summaries may serve as examples for security professionals considering ways to use metrics. Combining the summaries with scoring and expert reviews provides insights not only into the metrics, but also into the use of the Security MET.

These metrics measure a variety of issues and come from a variety of industries (as well as different countries).

Metrics Collected and Evaluated	
1. Office Space Usage Metric	9. Personnel Security Clearance Processing Metric
2. Security Activity Metric	10. Loss Reduction-Security Cost Metric
3. Environmental Risk Metric	11. Operations Downtime Reduction Metric
4. Averted External Loss Metric	12. Due Diligence Metric
5. Security Audit Metric	13. Shortage-Shrinkage Metric
6. Officer Performance Metric Panel	14. Phone Theft Metric
7. Security-Safety Metric	15. Security Inspection Findings Metric
8. Security Incident Metric	16. Infringing Website Compliance Metric

Sources of Metrics (Industries)	
Defense/Aerospace	Pharmaceutical
Energy/oil	Real estate management
Finance/banking	Retail
Government	Security services
Insurance	Shipping/logistics
Manufacturing/industrial products	Telecom

Some of the metrics are more sophisticated and detailed than others, providing a range of examples for potential users to consider. The metrics are not presented as models of perfection. Rather, they are authentic examples that security professionals can follow, refine, or otherwise adapt when developing their own metrics.

F. Presenting Metrics to Senior Management

A key task in this research was to develop guidelines for effectively using security metrics to persuade senior management. About 56 percent of survey respondents who use metrics share those metrics with senior management.

What would make those presentations more compelling? Several recommendations emerged:

- **Present metrics that are aligned with the organization's objectives or risks or that measure the specific issues in which management is most interested.** Experts advising the researchers emphasized the importance of focusing metrics on organizational risks and objectives, as

well as any other issues that are important to senior executives, especially return on investment (ROI).

- **Present metrics that meet measurement standards.** Because metrics are quantitative, they exude a scientific authority. However, if a metric is based on invalid or unreliable data, one cannot draw accurate conclusions from it and it will lack external credibility. A metric that has been properly designed from a scientific point of view and that has been evaluated against a testing tool (such as the Security MET) or established measurement and statistical criteria may appear more valuable and persuasive to senior management.

- **Tell a story.** If the metric is prevention-focused, a security professional can make the metric compelling by naming the business resources threatened, stating the value of those resources, and describing the consequences if the event occurs. Another part of a compelling story is the unfolding of events over time. Metrics can show progress toward a specific strategic goal. Incident management software may help make organizing and discerning meaning from data (i.e., trend analysis) faster and less burdensome. Benchmarking can enrich a story, but benchmarking depends on organizations' willingness to share their data, which they often decline to do.

- **Use graphics, and keep presentations short.** Persons interviewed for the metric summaries offered several tips: less is more; senior management likely care about only a few security metrics; if a security professional uses a dashboard to manage the metric, he or she should create an even simpler one for senior management; the presentation should run five minutes or less; and presenters should summarize findings and not bother executives with trivia.

- **Present metric data regularly.** Among those who share their metrics outside the security department, 40 percent do so monthly, 43 percent quarterly, and 17 percent annually. The research does not suggest an optimal interval for sharing security metrics with senior management. The survey shows that 83 percent of security professionals who share metrics outside the department do so at least quarterly. As data ages, it could become more historical, less actionable, and thus potentially less valuable. Distinguishing metrics that are time-sensitive from those that provide value over time will enhance the overall value of metrics.

G. Future Practitioner Needs

Possibilities include the following:

- **Larger metrics library.** This report presents 16 metric summaries, all of which have been evaluated by experts and researchers. It would be useful to discover, summarize, and evaluate more metrics and build a larger library that practitioners can consult. A larger library might also facilitate benchmarking.

- **Metrics training for security practitioners.** This could take the form of a video, a webinar, interactive online training, or an instructor-led module in a workshop or seminar. The training could teach security professionals how to use the Security MET, the database of metric summaries, and the guidelines for persuasive metric presentations. Successfully developed metrics could be included in a growing metrics library.

- **Follow-up contact with metric survey respondents who indicated they would like more information about metrics.**

- **Additional publications.** To spread the project's findings further, it could be useful to develop other publications from the research, such as magazine articles, journal articles, or handbooks.

- **Certification.** ASIS could consider developing a security metrics certification, along with metrics training. The subject of metrics could also be emphasized in Certified Protection Professional training and testing.

- **Metrics standard.** ASIS has produced numerous standards so far and could create a new standard on metrics development and use.

- **Tool for creating a metric from scratch and implementing it in an organization.** The present research focused on helping security professionals discover existing metrics, evaluate them in order to improve and adapt them, and present them to senior management effectively. Another research project could take a different approach, attempting to develop a detailed yet simple fill-in-the-blanks template that practitioners could use to develop and implement a metric from scratch. A further possibility is to design a software application to create, collect, and store metrics using a dashboard model.

- **Audited metrics.** The current metric summaries are based on descriptions provided by the metric users. A deeper level of research would obtain the fine details of a metric and subject it to an outside audit. That approach could lead to a highly detailed account of a metric's creation, use, and impact in a particular setting.

The complete project report contains the full text of the Security MET, the library of metric summaries (with evaluations), the literature review, and the results of the online survey.

I. Purpose and Sponsorship of This Research

Security metrics support the value proposition of an organization's security operation. Without compelling metrics, security professionals and their budgets continue largely on the intuition of company leadership. With metrics, the security function grounds itself on measurable results that correlate with investment, and the security professional can speak to leadership in a familiar business language. Security metrics are vital, but in the field and in the literature one finds few tested metrics and little guidance on using metrics effectively to inform and persuade senior management.

To address the gap, in spring 2013 the ASIS Foundation sponsored a major research project designed to add to the body of knowledge about security metrics and to empower security professionals to better assess and present metrics. The Foundation awarded a grant to Global Skills X-change (GSX), partnered with Ohlhausen Research, to carry out the work. The project's main objective was to develop a tool to help security professionals evaluate metrics. Once evaluated, the metrics can be improved and more effectively used to demonstrate return on investment or support other organizational goals. It was understood that, to be effective, any study on metrics must be generalizable internationally across all industries. The study met that requirement through its broad data-collection strategy.

With advice from the project's advisory board and expert panel, the research team conducted an extensive literature review; collected data through an online survey, telephone interviews, and an advisory board and expert panel; and developed and refined an evaluation tool for users. This report provides the project's findings, including the project's three practical, actionable products:

- The Security Metrics Evaluation Tool (Security MET), which security professionals can self-administer to develop and improve security metrics

- A library of metric descriptions, each evaluated according to the Security MET criteria

- Guidelines for effective use of security metrics to inform and persuade senior management, with an emphasis on organizational risk and return on investment

- The research aimed for generalizability of results. Therefore, the survey sample, follow-up interviews, research team, advisory board, and expert panel included persons from a wide range of industries and fields, as well as a range of countries.

The research team wishes to thank the ASIS Foundation for its generous support of this work.

II. Methodology

In spring 2013, the ASIS Foundation contracted with Global Skills X-change (GSX) to perform this research. GSX specializes in applying validation, measurement, and standards development techniques to produce business tools. GSX subcontracted with Ohlhausen Research, Inc., which focuses on research in security, criminal justice, and technology. Project work began on June 1, 2013.

A. Personnel

The research team included the following:

- **Principal Investigator:** Peter Ohlhausen, President, Ohlhausen Research, Inc. A researcher in the security field for more than 25 years, Mr. Ohlhausen has assisted in the multi-year revision of *Protection of Assets*, served as senior editor of *Security Management* magazine, and conducted numerous research and consulting projects for the U.S. Department of Justice, U.S. Department of Homeland Security, ASIS, and corporate clients.

- **Subject Matter Expert:** Daniel McGarvey, Director, Security Programs, GSX. Mr. McGarvey has more than 30 years of experience managing and directing national and international programs requiring sensitive compartmented information and special access in government and industry. An experienced chief security officer (CSO), he rebuilt the security infrastructure for the Department of the Air Force.

- **Technical Advisor:** Lance Anderson, PhD, Workforce Solutions Practice Director, GSX. Dr. Anderson has more than 20 years of experience conducting and directing research focused on developing and evaluating performance metrics, often in security environments. He has published and presented numerous times on occupational analysis, utility analysis, and data collection and analysis techniques.

- **Senior Analyst:** Megan Poore, MS, Research and Workforce Analyst, GSX. Ms. Poore has been a key contributor in certification program development, including assessment development and psychometric analyses. She also has expertise in conducting occupational analyses, developing competency models, and managing competency model survey analyses for numerous occupations.

The project gained valuable advice from two outside groups of security professionals experienced in the use of metrics. The *advisory board* provided general guidance on the project and helped in developing the Security Metrics Evaluation Tool (Security MET). The *expert panel* provided insights on the Security MET and reviewed the metrics summaries developed through phone interviews. Members of the advisory board and expert panel are listed in the acknowledgments at the front of this report. The final project report (this document) benefited from careful review by members of the ASIS Foundation Research Council.

B. Major Research Tasks

The main tasks were as follows:

1. **Review and summarize the current literature on the use of security metrics to inform and persuade corporate management.** The review cites nearly 100 sources and provides a comprehensive review of the current state of metric development and application.

2. **Develop and refine a Security Metrics Evaluation Tool (Security MET).** The Security MET is a written tool that security managers can use to assess the quality of specific security metrics. The tool was revised throughout the research process, based on feedback from the advisory board and expert panel.

3. **Collect qualitative data to identify and evaluate current practices in the use of security metrics.**

   a. *Online survey.* More than 3,000 ASIS members were asked to participate in an online survey. Invitations were sent to all ASIS council members and the CSO Roundtable, plus an ASIS-created pool of top-level security professionals. A total of 297 people participated in the survey.

   b. *Interviews.* The team conducted detailed follow-up interviews, mostly by telephone, with survey respondents who indicated that they had successfully used security metrics to inform and persuade corporate management. The interviews led to detailed summaries of 16 security metrics that are actually in use in the field.

   c. *Metric review.* The research team had each metric summary reviewed and scored by two expert panel members and one member of the research team. The reviewers assessed the metric summaries by applying the Security MET.

C. Deliverables

The research project was tasked with providing three practical, actionable products:

1. **Security MET.** This written tool, provided in Appendix A, asks the user to rate a metric based on nine criteria. The criteria are grouped in three categories:

   Technical Criteria – Category 1

   1. Reliability
   2. Validity
   3. Generalizability

   Operational (Security) Criteria – Category 2

   4. Cost
   5. Timeliness
   6. Manipulation

Strategic (Corporate) Criteria – Category 3

7. Return on Investment

8. Organizational Relevance

9. Communication

Each criterion is explicitly defined. On a scale of 1 to 5, the user rates the metric based on each criterion, using the supplied anchors and definitions. A score sheet is presented at the end. The scoring process helps the user determine the relative strong and weak points of a given metric. For example, the metric might score high on strategic criteria but low on technical criteria. In that case, the user could consider ways to strengthen the metric's reliability, validity, or generalizability.

2. **Database of selected security metrics.** The project report contains 16 metric summaries (Appendix B), each evaluated by three reviewers according to the Security MET criteria. These are metrics in actual use today. They measure a wide variety of issues and come from a wide variety of industries (as well as several different countries). Some of the metrics are more sophisticated and detailed than others, providing a range of examples for potential users to consider.

Metrics Collected and Evaluated	
1. Office Space Usage Metric	9. Personnel Security Clearance Processing Metric
2. Security Activity Metric	10. Loss Reduction/Security Cost Metric
3. Environmental Risk Metric	11. Operations Downtime Reduction Metric
4. Averted External Loss Metric	12. Due Diligence Metric
5. Security Audit Metric	13. Shortage/Shrinkage Metric
6. Officer Performance Metric Panel	14. Phone Theft Metric
7. Security-Safety Metric	15. Security Inspection Findings Metric
8. Security Incidents Metric	16. Infringing Website Compliance Metric

The metrics are not presented as models of perfection. Rather, they are authentic examples that security professionals can follow, refine, or otherwise adapt when developing their own metrics.

3. **Guidelines for effective use of security metrics to demonstrate return on investment.** Chapter VII of this report presents guidelines gathered from a variety of sources: the literature review, the online survey, the follow-up telephone interviews, the advisory board, and the expert panel.

III. Literature Review Highlights

Project staff performed an extensive literature review to inform the present research and to help security professionals gain a view of metrics currently in use, evaluate metrics, and persuasively present metrics to senior management. The full text of the literature review is presented in Appendix C. This section presents highlights.

Metrics drive business decisions and behavior. They influence process assessment and controls, business policies, collaboration for enterprise-wide benefits, business investment decisions, and strategic and profit center alignment. However, the literature review identified a lack of explicitly defined metric criteria, evidence needed to document that the criteria were met, and sample metrics that meet the criteria. Valid and reliable metrics lead to more accurate conclusions and more persuasive communication with senior management.

Metrics allow organizations to hold individuals accountable for specified results and goals, and they are a vehicle through which security programs can demonstrate their measurable impact on an organization's strategic, organizational, financial, and operational risks and profits (Campbell, 2007).

A. Introduction

Metrics enable process assessment and controls, drive business policies and investment decisions, influence collaboration for enterprise-wide benefits, and motivate strategic and profit center alignment. Security metrics are vital, but the field offers few tested metrics and benchmarks (Guidelines and Metrics Working Group, ASIS Defense and Intelligence Council, 2012). With a significant rise in the availability and use of big data (i.e., datasets that are so voluminous that the ability to structure, process, and comprehend the data is arduous), it is imperative that organizations select the right metrics.

Historically, there has been a disconnect between security programs and the core businesses they serve. However, the risk environment has dramatically changed within the last 30 years, in part due to new avenues in technology (Campbell, 2006). Security programs must now gauge their effectiveness in terms of risk mitigation and do so in a way that speaks to senior executives. Metrics are a vital tool for this gauge, and, as such, the perceived value of metrics is on the rise (Campbell, 2007).

For example, in "Make Better Decisions," Davenport (2009) describes the benefits of metrics. Davenport uses the term "analytics" to describe decision-making driven by quantitative analysis and data. When a company uses metrics or analytics, the decisions made are more likely to be the right ones, as these decisions are grounded in the scientific method.

The literature defines metrics in various ways. An old definition of security metrics from Carnegie Mellon University (1995) states:

> Metrics are quantifiable measurements of some aspect of a system or enterprise…. Security metrics focus on the actions (and results of those actions) that organizations take to reduce and manage the risks of loss of reputation, theft of information or money, and business discontinuities that arise when security defenses are breached.

This definition can be broadened to include the protection of people, property, and information. Security metrics are a crucial aspect of risk management (Azuwa, Ahmad, Sahib, & Shamsuddin, 2012). In the information security field, researchers have defined metric in numerous ways (Azuwa et al., 2012):

- a measurement that is compared to a scale or benchmark to produce a meaningful result

- a quantitative and objective basis for security assurance, comparing two or more measurements taken over time with a predetermined baseline

- an indicator, not an absolute value with respect to an external scale

- a measurement standard that can be quantified and reviewed to meet security objectives, facilitate relevant actions for improvement, and aid decision making and compliance with security standards

The term *metrics* is sometimes used interchangeably with measurements, analytics, and performance metrics throughout the security literature.

B. Existing Security Metrics

The most thorough metric review to date was done by Campbell (2007); he describes metrics as falling into numerous categories, such as key performance indicators, risk analyses, and diagnostic measures. Security metrics have also been categorized based on security type, including human resources/personnel security, physical security, industrial security, information and cyber security, etc. (Guidelines and Metrics Working Group, ASIS Defense and Intelligence Council, 2012). Business function is an additional framework used to explore metrics. Metrics can also be explored based on their degree of automation, such as metrics obtained from an incident management system (McIIravey & Ohlhausen, 2012).

Key performance indicators (KPIs) are a type of metric; KPIs are established by identifying a desired performance level and assessing the progress, or lack thereof, toward that level (Campbell, 2007). Examples of KPIs include employee and customer satisfaction surveys, the number of shipped goods that arrive to their destination intact, and the number of information security events that occur within a year (Mayor, 2006; Pironti, 2007).

Risk analyses are another category of metric. They may involve measuring assets in terms of cost of loss or loss events, or conducting a cost-benefit analysis (Campbell, 2007). Baseline performance metrics can also be valuable; emergency service response time would be an example of a baseline performance metric. Diagnostic metrics involve identifying the root causes of trends; for example, an organization might examine the causes of increased workplace violence incidents in a specific branch.

Security metrics are often categorized based on the type of security (human resources or personnel security, physical security, industrial security, information and cyber security, etc.) in which they are used. Human resources or personnel security addresses measurable issues including compliance, cost controls and efficiency, and continuous evaluation (Guidelines and Metrics Working Group, ASIS Defense and Intelligence Council, 2012).

Physical security metrics include measureable issues surrounding alarms, protective barriers, theft, etc. Garcia (2008) writes:

> The performance measures for a PPS [physical protection system] function include probability of detection; probability of and time for alarm communication and assessment; frequency of nuisance alarms; time to defeat obstacles; probability of and time for accurate communication to the response floor; probability of response force deployment to adversary location; time to deploy to a location; and response force effectiveness after deployment.

These measures or metrics play an important role in meeting the objectives of a physical protection system (Garcia, 2008) and are also useful in vulnerability assessment (Garcia, 2006).

Other physical security metrics include the number of patients searched by emergency services at a hospital, the number of armed robberies at a specific store location, and inventory shrinkage (Health Resource Network, Inc., 2000; Wailgum, 2005). The number of door alarm annunciations is another physical security metric. It has been used to explore the cause of false alarms so that all alarms do not have to be treated as emergency security situations (Treece & Freadman, 2010).

The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard (Interagency Security Committee, 2013) recognizes security metrics as an important component of risk management. Pursuant to Executive Order 12977, the standard sets policy that requires federal entities to assess and document the effectiveness of their physical security programs through performance measurement and testing (metrics).

The security domain that has the greatest presence in the metrics literature is by far information and cyber security. International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 27001 is a widely used, best practice certification that outlines information technology security standard requirements surrounding the range of threats and vulnerabilities. The ISO/IEC 27001 standard mandates the measurement of information security as a requirement (Azuwa, Ahmad, Sahib, & Shamsuddin, 2012). In addition, the ISO/IEC 27002 standard dictates security techniques for managing information security (ISO/IEC, 2005b).

Metrics can also be organized by business function. Metrics in this category include security cost per employee and annual security costs in relation to annual revenue (McIIravey & Ohlhausen, 2012).

Return on investment can also serve as a framework for categorizing metrics. A Global Information Security Survey was conducted by *Information Week* and Accenture on more than 1,100 professionals in the field of business technology ("Gauging security ROI," 2007). The following are their answers to the question "How does your company measure the value of your security investments?"—in other words, where is your ROI?: fewer worker hours spent on security-related issues; better protection of customer records; decline in breaches; decline in amount of network downtime; improved protection of intellectual property; better risk-management strategies; and reduction in incident-response time. Without metrics it may be impossible to show the security function's value in a form that business leaders will understand (Gill, Burns-Howell, Keats, & Taylor, 2007).

Some metrics are captured instantaneously through incident management software (IMS), such as the IMS used in emergency preparedness (McIIravey & Ohlhausen, 2012; Dallas county uses DHS grant to grab incident management software, 2008). IMS from iViewsystems is currently being used

at Hershey Entertainment & Resorts to manage security metrics, such as employee injuries, and to document and share data (Case study: Hershey Entertainment & Resorts, n.d.). Delta Air Lines uses Perspective from PPM 2000 to track compliance issues, accidents, medical emergencies, and financial crimes; the metrics then lead to policy recommendations both inside and outside the security department (McIIravey & Ohlhausen, 2012). Advanced data collection may also facilitate benchmarking and a more standardized approach to security return on investment.

The complete literature review (in Appendix C) includes a list of 36 metrics, which are examples of metrics discovered during the literature review process.

C. Metrics Communication

Communicating metric value remains a challenge. It does not matter how great the data is if it cannot be understood by key stakeholders (Dix, 2013). Corporate management tends to view security as overhead (i.e., a cost center rather than a production center) and security metrics as merely measuring activity, not value. Security professionals note that security benefits are difficult to measure compared to the benefits of profit centers, and such professionals often lack the skills or time to create and administer effective metrics. Thus, current security metrics, in practice, are generally not compelling and are often not taken seriously (Rothke, 2009). However, the literature offers suggestions for improving metric communication.

Benchmarking allows organizations to see where they stand on a given metric in relation to their competitors; unfortunately, this approach is contingent on the widespread use of identical metrics and organizations' willingness to share their data. Communicating metrics based on return on investment is another tactic used to illustrate the importance of the data being collected; however, this calculation is not straightforward.

One technique for communicating metric results is to tailor the communication to the audience. Security professionals should define their metric values in terms that management will understand (Ting & Comings, 2010). Also, one can be more persuasive by using metrics to tell a story—that is, by collecting metrics that are forward-looking and backward-looking and by addressing the questions "Where are we going?" and "Where have we been?" (Campbell, 2011; Blades, 2012). Security professionals can best explain their findings by providing specific, concrete examples that are meaningful to the audience (Deming, 2012).

Another method is to focus on risks—to discuss metrics in terms of the probability of future events and the severity of the consequences if these events occur (Doinea & Pavel, 2010; Azuwa, Ahmad, Sahib, & Shamsuddin, 2012). When discussing and presenting risk-based data, it is important also to disclose the inherent uncertainties of the metrics used. Managers factor uncertainties into their daily decision making; not communicating uncertainties leads to perceptions of dishonesty (Refining risk management, 2011). Security professionals are also advised to talk specifically about the actual business resources threatened and the value of these resources (Brenner, 2010). According to "Leveraging Corporate Security for Business Growth and Improved Performance: The Transformative Effect of 9/11" (2012), by the Conference Board Council of Corporate Security Executives, the International Security Management Association, and the CSO Roundtable of ASIS International, corporate business units "ultimately own the risk, with security as a critical partner, identifying those risks and developing ways to manage them."

A final method is to measure and communicate metric results over time. Ultimately, metrics are the marketing tool for the security program (McIIravey & Ohlhausen, 2012). Examining metric trends over time allows for meaningful comparisons to be made and can be a useful vehicle for communicating metric value and results. Metrics should be communicated in terms of the strategic goal they are linked to; progression toward this goal should be measured over time (Drugescu & Etges, 2006; Enescu, Enescu, & Sperdea, 2011). Incident management software (IMS) can help make organizing and discerning meaning from data (i.e., trends analysis) faster and less burdensome on personnel, and thus could serve as a crucial aid in efficient and effective communication (McIIravey & Ohlhausen, 2013).

D. Metrics Evaluation

The security literature discusses many factors that should be examined when determining the effectiveness of a metric, including ROI, metric type, data automation, SMART criteria, relevance to organizational objectives, etc. However, it is important to note that these factors are generally presented only at a conceptual level within the security literature. Definitions that yield specific measurements are not provided; the evidence needed to show that these factors are met is not discussed; examples of metrics that illustrate the desired measurement criteria are not found.

In addition, explicit empirical evidence regarding security metric validity and reliability is absent from the security literature. If a metric is not reliable or valid, then the conclusions drawn from it will be inaccurate. For example, if the number of door alarm annunciations increases tenfold in one month, a security professional might conclude that this represents an increase in attempted burglaries; however, this increase could merely be due to a faulty door alarm system. Drawing inaccurate conclusions and communicating misinformation would undermine the security professional's attempt to describe and improve security, which in turn would drive management to further underestimate the importance of security and security metrics.

E. Conclusion

Without compelling metrics, security professionals and the budgets that power their operations continue largely on the intuition of company leadership. With metrics, the security function grounds itself on measurable results that correlate with investment, and the security professional can speak to leadership in a familiar business language.

Overall findings from the literature:

- Descriptions of existing security metrics are often vague, making it difficult to adopt those metrics. The focus is more on counting events than creating meaningful, risk-based metrics.

- Strategies for communicating metrics are general and may be hard to implement.

- Typically, evaluation criteria are only presented at a conceptual level within the security literature, without explicit definitions.

- Few examples of empirically sound metrics (with statistical justification and evidence) are present within the security literature. Physical security and information security appear to have more metrics in use than other security fields.

IV. Development of Security Metrics Evaluation Tool (Security MET)

The Security Metrics Evaluation Tool (Security MET) is a written tool that security managers can use to assess the quality of specific security metrics. Users will be able to determine whether an existing or proposed metric possesses scientific validity, organizational relevance (such as clear alignment with corporate risks or goals), return on investment, and practicality. Basically, the tool was designed to help a user identify a metric's strengths and weaknesses so that the weaknesses can be corrected. The Security MET is presented in Appendix A.

The tool was developed through a lengthy, iterative process that involved synthesizing scientific literature, security industry standards, and input from metrics experts in the project's advisory board and expert panel. To develop the criteria (the characteristics that make an empirically sound security metric), the research team turned to measurement and testing literature, as well as industry benchmarks, and developed criteria in three categories: technical, operational, and strategic. The team then consulted the project's advisory board. With the board's guidance, the research team refined the criteria, arriving at the final nine criteria (with three in each category). The Security MET was further evaluated and refined after members of the expert panel used it to evaluate the project's 16 metric summaries.

The final version includes the following criteria for evaluating a security metric:

Technical Criteria – Category 1

    1. Reliability

    2. Validity

    3. Generalizability

Operational (Security) Criteria – Category 2

    4. Cost

    5. Timeliness

    6. Manipulation

Strategic (Corporate) Criteria – Category 3

    7. Return on Investment

    8. Organizational Relevance

    9. Communication

Category 1 (Technical Criteria) includes reliability, validity, and generalizability. Reliability (criterion 1) is the degree to which the metric yields consistent scores that are unaffected by sources of measurement error (e.g., the time when the measure was taken, the identity of the raters, the weather that day). Validity (criterion 2) refers to the degree to which evidence based on theory or quantitative research (conducted by the user or others) supports drawing conclusions from the metric. The *Principles for the Validation and Use of Personnel Selection Procedures* (2003) and the *Standards for Educational and Psychological Testing* (1999) provide guidance on the sufficiency and types of

validity and reliability evidence that should be collected. Validity can also be illustrated through the generalizability of the measure to other situations, samples, tests, etc. (Straub, Hoffman, Weber, & Steinfield, 2002). Generalizability (criterion 3) is the degree to which conclusions drawn from the metric are consistent and applicable across different settings, organizations, timeframes, or circumstances in addition to the extent to which metric results allow for external comparison across organizations.

Category 2 (Operational (Security) Criteria) includes cost, timeliness, and manipulation. Cost (criterion 4) is defined as the monetary and non-monetary costs associated with metric development and administration, as well as negative consequences associated with the metric. Examining metric budgets and inputs is a common factor to consider when choosing and evaluating metrics (Martin, Bulkan, & Klempt, 2011; Hastings, 2013). Timeliness (criterion 5) is defined as the extent to which metric data can be gathered in a timely fashion so the results can have an impact. Timeliness of metric data, relating to the ease and automation of data, can help determine metric effectiveness (Azuwa, Ahmad, Sahib, & Shamsuddin, 2012). Manipulation (criterion 6) refers to the extent to which metric data cannot be coached, guessed, or faked by staff, and the extent to which metric has built-in data quality checks or oversight. The *Principles for the Validation and Use of Personnel Selection Procedures* (2003) and the *Standards for Educational and Psychological Testing* (1999) highlight the importance of metrics being devoid of measurement error.

> ### Psychometric Basis of Security MET
>
> To identify ways to evaluate and enhance security metrics, we conducted a literature search regarding broad measurement techniques and theory. We found that psychometric research was most valuable.
>
> Psychometrics is the field concerned with the measurement of mental traits, abilities, and processes. The psychometric literature includes the measurement of behaviors and social science research criteria.
>
> There are several reasons why the psychometric literature is particularly applicable to the challenges of developing and maintaining security metrics. In particular, the psychometric literature addresses the measurement of complex human behaviors, including the various sources of error inherent in social and organizational situations. In addition, through its connection with legal guidelines and case law, psychometric theory provides ways to address complicated legal issues related to fairness and human error.

Category 3 (Strategic (Corporate) Criteria) includes return on investment (ROI), organizational relevance, and communication. Return on investment (ROI) (criterion 7) is the extent to which a metric can be used to demonstrate cost savings or loss prevention in relation to relevant security spending. This involves expressing the following in terms of dollars or some other unit relevant to decision makers: the cost of the security intervention, the effects of the security intervention, and any unintended consequences directly related to the intervention. ROI can be a vehicle for metrics to justify budgets and can help in examining financial inputs and outputs of various security activities; these factors are of utmost importance to management and key stakeholders (Martin, Bulkan, & Klempt, 2011; Hastings, 2013). Organizational relevance (criterion 8) is the extent to which the metric is linked to organizational risk management or a strategic mission, objective, goal, asset, threat, or vulnerability relevant to the organization—in other words, linked to the factors that matter most to senior management. Metrics should be evaluated in terms of their relevance to high-level organizational objectives and should be tailored to address a specific business need (Prince,

2009; Rathbun, 2009). Communication (criterion 9) refers to the extent to which the metric, metric results, and metric value can be communicated easily, succinctly, and quickly to key stakeholders, especially senior management. It does not matter how great the data is if it cannot be understood by key stakeholders (Dix, 2013).

For each criterion, the Security MET presents a definition, concept illustration, behavioral summary scale, and sample applications. Definitions are presented in the paragraphs above. A concept illustration is presented following each definition; this illustration provides a familiar, everyday example of what would indicate a high and low level of the criterion. A behavioral summary scale is then presented. Each criterion is scored using a behavioral summary scale ranging from 1 to 5. The behavioral summary scale presents examples of behaviors, ranging from lower to higher criterion levels, and allows the user to choose a number from along that range that best corresponds with his or her metric. Anchors 1, 3, and 5 are defined using behaviors; 2 and 4 are appropriate when the reality lies between two anchor definitions. Sample applications are then presented following the behavioral summary scale; these serve as examples to help users better understand how a metric should be scored on the criterion. A criterion from category 3 (strategic or corporate criteria) is presented as an example:

Criterion 8: Organizational Relevance

Extent to which metric is linked to organizational risk management or a strategic mission, objective, goal, asset, threat, or vulnerability relevant to the organization— in other words, linked to the factors that matter most to senior management.

Illustration of the concept:

> *An organization has a goal of reducing the weight of the object it manufactures. If a scale is used to calculate the weight of manufactured products, this metric would be of high organizational relevance based on its linkage to the goal. In contrast, if a person measured the length of the object, the measurement would be of low organizational relevance.*

Please rate the metric on the following scale. Read the description of each level and select the number that most closely corresponds to the metric. Mark the score on the score sheet at the end of this tool.

1 = low organizational relevance, 5 = high organizational relevance

The metric is **not linked** to a specific organizational strategic mission, objective, goal, asset, risk, threat, or vulnerability; if linked, the linkage is **weak** and of **minimal relevance** to the organization; the data derived from this metric is of **little importance** to senior management.		The metric is **somewhat linked** to a specific organizational strategic mission, objective, goal, asset, risk, threat, or vulnerability; the linkage is **moderate** and of **some relevance** to the organization; the data derived from this metric is of **some importance** to senior management.		The metric is **explicitly linked** to a specific organizational strategic mission, objective, goal, asset, risk, threat, or vulnerability; the linkage is **strong** and of **high relevance** to the organization; the data derived from this metric is of **great importance** to senior management.
1	2	3	4	5

Sample Application:

Metric: Number of thwarted hacking attempts against company's cloud-based software.

Example Score: A software company supplies a cloud-based application to its customers. A vital goal of the company is to keep the application properly functioning and available to clients 99.99 percent of the time. Therefore, a metric regarding the number of denial-of-service attacks

thwarted through security efforts would be highly relevant to the organization's goals and would likely be of interest to senior management. As a result, the metric would receive a 5 on this criterion.

Scores on the Security MET are obtained by summing the chosen rating for each criterion within each category and then across categories. The team considered including a weighting component to the Security MET score. However, feedback and further consideration led to a removal of the weighting system, following the conclusion that the criteria that are of most importance to a metrics user may depend on the context (e.g., budget concerns, senior management buy-in concerns). A score sheet is presented at the end of the Security MET to tabulate the metric's score across the nine criteria. Lower scores on particular criteria show where a metric has room for improvement.

The Security MET is designed to help the user review and understand all the behaviors associated with the criteria at varying levels. It establishes a common frame of reference for individuals to use when examining and rating their metrics. This frame of reference is further reinforced by the examples presented that highlight how a metric should be scored based on the criteria presented. Finally, the instrument is easy to score, imposes little to no time burden on staff, and could easily be placed on a wide variety of online systems.

V. Online Survey Highlights

On August 7, 2013, with the help of ASIS International and in concert with the ASIS Leadership & Management Practices Council, the research team invited more than 3,000 ASIS members to participate in an online survey. Invitations were e-mailed to all ASIS council members and the CSO Roundtable, plus an ASIS-created pool of top-level security professionals.

Specifically, the ASIS IT Department pulled the names of all ASIS council members (775), all CSO Roundtable members (320), and all ASIS members with titles of "director" and above (4,521). The pool was selected as being more likely to include metrics users (compared to a random sample of ASIS members). After the list was deduplicated and corrected, a link to the survey was e-mailed to 3,304 individuals. Of the e-mails sent, 95 percent were successfully delivered. Of those, 22 percent were opened. Of those opened, 43 percent led to survey participation. A total of 297 people responded to the survey.

This data collection process was not designed to determine the prevalence of security metrics use in the security profession generally (e.g., to learn that 22 percent of security managers use security metrics). Instead, it was designed to uncover specific instances of security metrics use (for follow-up interviews) and gain an understanding of the different ways in which security professionals may be using metrics.

This section presents survey highlights. Complete survey results, including detailed, open-ended responses, are presented in Appendix D.

The survey contained the following questions:

Survey Questions	
Q1: Collection And Use Of Security Metrics	Q10: Metric Elements Shared With C-Suite Personnel
Q2: Metric Comparison To External Benchmarks	Q11: Most Important Metrics – Senior Management
Q3: Would You Use Metrics?	Q12: Most Important Metrics – Why?
Q4: Measured Security Program Aspects	Q13: Metric Alignment With Risk/ Objectives
Q5: Who Records Metrics?	Q14: Metric Alignment With Risk/ Objectives – How?
Q6: Metrics Provisions To Non-Security Persons	Q15: Dashboard Tool Usage
Q7: Metrics Provisions To Non-Security Persons – If No, Why Not?	Q16: Who Developed Dashboard Tool?
Q8: Metrics Provisions To Non-Security Persons – Who?	Q17: Third-Party Dashboard Tool Name
Q9: Metrics Provisions To Non-Security Persons – How Often?	Q18: Metrics Interview Volunteers
	Q19: Work Region
	Q20: Desire Information Regarding Metrics

Overall, respondents were generous with their time and insights, providing the research team with a detailed view of the many ways in which security professionals are using metrics today. Their conscientious participation in the survey shows a high degree of interest in the topic of metrics:

- Seventy-seven percent of respondents said they are collecting and using security metrics.
- Of respondents who said they are not using security metrics, 78 percent said they would use metrics if they knew more about how to create them and use them effectively.
- Out of all respondents, 55 percent said they would like to receive more information from ASIS regarding metrics and supplied their names and e-mail addresses.
- Remarkably, 40 percent of respondents using metrics said they would be willing to speak to a researcher by phone about their use of metrics.

The remaining percentages refer to respondents who said they are using metrics:

- **Benchmarks.** Only 39 percent compare their metrics to external benchmarks. Benchmarks in use included such items as industry figures on turnover and training, competitors' metrics, crime statistics, government benchmarks, industry reports, and published standards.
- **Metrics topics.** Respondents were asked which aspects of the security program are measured to determine current performance levels or program effectiveness. They were given a list of 13 categories (plus "other") and asked to check all that apply. The top five categories of metric focus were security incidents, criminal incidents and investigations, cost against budget, security training and education, and guarding performance (turnover, inspections, etc.).
- **Data collection.** Seventy-eight percent said their metrics were recorded by an internal security department manager or specialist.
- **Sharing and reporting.** Eighty percent provide their metric findings to persons outside the security department. Recipients of the information include senior management (listed by 79 percent of those who share metrics outside the security department), managers of other departments (59 percent), supervisors (51 percent), and people who report to the security department (47 percent). Those who share metrics provide the information quarterly (43 percent), monthly (40 percent), or annually (17 percent).

Does security provide these metrics to persons outside the department?

19.6

80.4

Yes
No
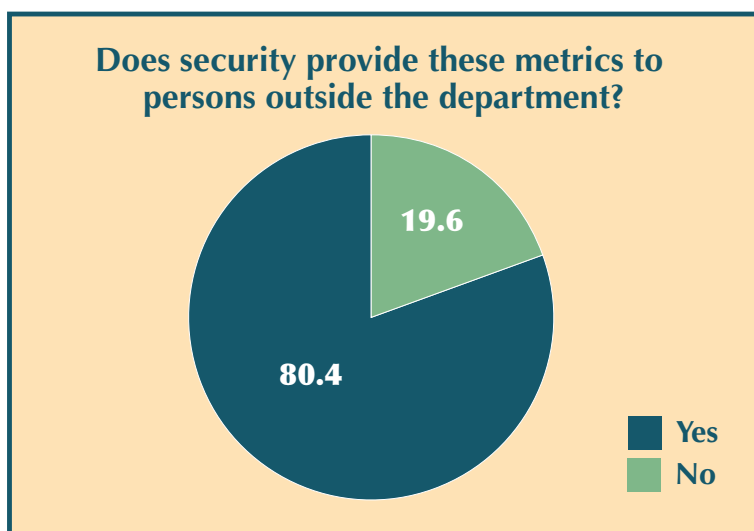
Those who do not share metrics outside the department listed various reasons centered on privacy, confidentiality of operations, and lack of external interest.
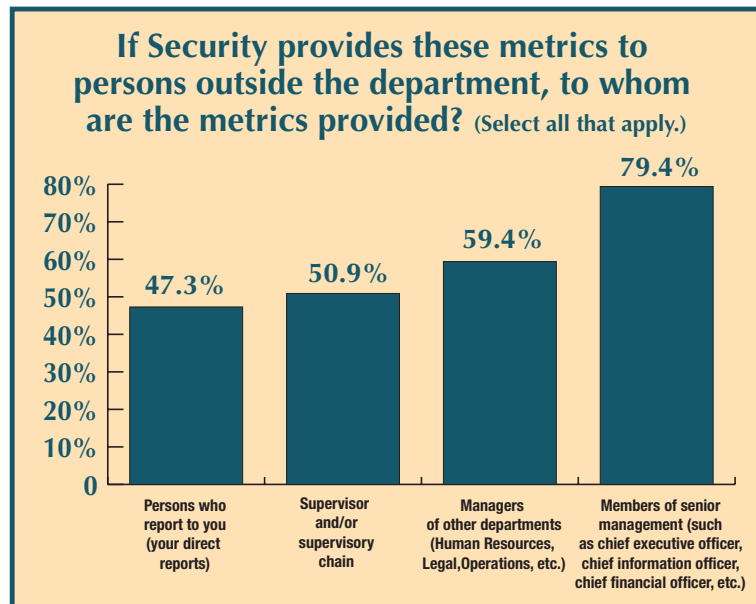
If Security provides these metrics to persons outside the department, to whom are the metrics provided? (Select all that apply.)

- **Topics shared with C-suite.** Respondents who share metrics with C-suite personnel were given a list of 13 categories of topics (plus "other") and asked which elements they share (selecting all that apply). The top choices were security incidents (80 percent), cost against budget (62 percent), criminal incidents and investigations (57 percent), regulatory compliance (44 percent), and risk analysis process (40 percent).

- **Metrics most important to senior management.** When asked which elements or metrics senior management considers most important, 38 percent of respondents named metrics in the category of finance, and 26 percent named metrics in the security incidents/safety considerations category.

- **Alignment with organizational risk or objectives.** Seventy percent of respondents who use metrics said their metrics are tied to, aligned with, or part of the larger organizational risk process or organizational objectives.

Are your metrics tied to, aligned with, or part of the larger organizational risk process or organizational objectives?
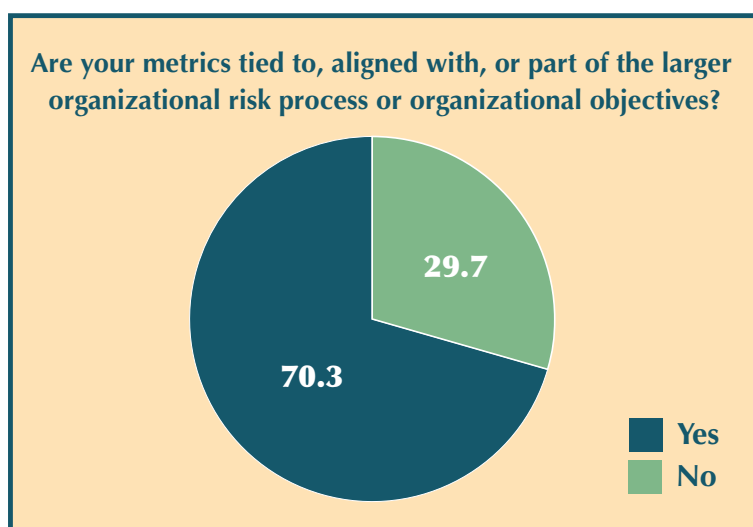
Those who answered "yes" offered a range of explanations of how the metric is aligned with organization risk or objectives, such as the following:

- Our metrics are part of the continuous improvement program.

- Security is tied to many business units through such issues as risk, business continuity, travel, crisis management, compliance, investigations, major events, pre-employment background investigations, executive protection, and intelligence analysis.

- We report our results to the risk department, which creates risk assessments for the entire business.

- We use metrics to show how security can help make the business more effective. Security is not just a line item expense.

- Our metrics are fully integrated into the enterprise risk management process.

- Our metrics are tied to the company's overall client satisfaction levels, differentiating us from our competitors. All other things equal, if we are more secure than our competitors that will improve business.

- The security goals derive from the business plan.

- Security is a business function tied into the bottom line of the enterprise.

- **Dashboard tool.** Only 44 percent of respondents using metrics perform their data collection, review, or sharing via a security management dashboard tool.

Are metrics collected, reviewed, or shared via a security management dashboard tool?

43.9   56.1

■ Yes
■ No
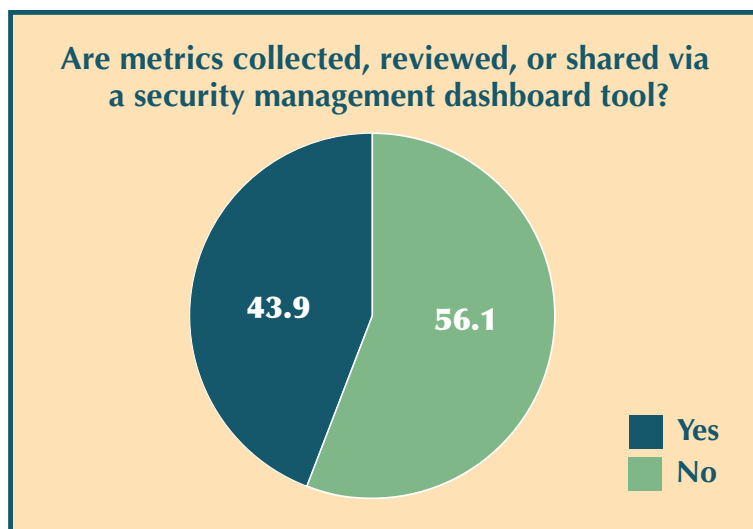
Of those who use a security management dashboard tool, 71 percent developed it in-house. Only 29 percent used a tool from a third-party provider.

- **Geographic spread of survey.** Survey participants came from around the world:

In which region do you primarily work?
(Select only one.)

Pie chart values:
- North America: 76.7
- South/Central America: 3.6
- Africa: 3.2
- Asia: 3.2
- Middle East: 1.6
- Australia & Oceania: 1.6
- Europe: 10.0

Legend:
- North America
- South/Central America
- Africa
- Asia
- Middle East
- Austrailia & Oceania
- Europe
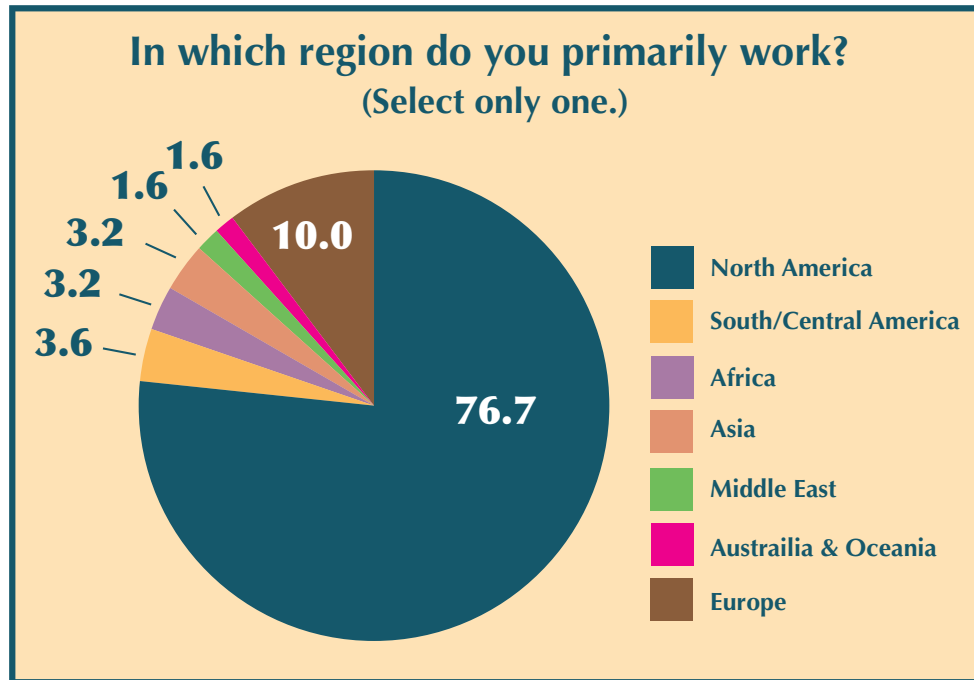
VI. Sample Metric Summaries and Ratings

The researchers developed 16 summaries of metrics in use in the security field as of 2013. The summaries were developed primarily through telephone interviews. Participants were identified through the project's online survey, which asked respondents if they were currently using metrics and would be willing to describe their practices to a researcher. About half the interviewees also supplied examples of the graphics they use to convey their metrics to senior management. All 16 summaries are presented in Appendix B, along with evaluations.

This section presents three examples from the library of 16. After each metric summary comes an evaluation. Each metric was scored against the Security Metrics Evaluation Tool (Security MET) by two to three members of the project's expert panel and one member of the research team. The outside experts are high-level security professionals who currently use metrics, and the researcher was especially well-equipped to focus on each metric's methodological (technical) aspects. Their scores are presented in a score sheet. The two outside experts reviewing each metric also supplied written comments about the metric. Those comments are condensed and provided below the score sheets. The scoring and written evaluations are meant to help readers see where they might strengthen any of these metrics if they chose to develop metrics for their own organizations.

The summaries that follow may serve as examples for security professionals considering ways to use metrics. Combining the summaries with scoring and expert reviews provides insights not only into the metrics but also into the application of the Security MET.

These are metrics in actual use today. They measure a wide variety of issues and come from a wide variety of industries (as well as several different countries). Some of the metrics are more sophisticated and detailed than others, providing a range of examples for potential users to consider.

Metrics Collected and Evaluated	
1. Office Space Usage Metric	9. Personnel Security Clearance Processing Metric
2. Security Activity Metric	10. Loss Reduction/Security Cost Metric
3. Environmental Risk Metric	11. Operations Downtime Reduction Metric
4. Averted External Loss Metric	12. Due Diligence Metric
5. Security Audit Metric	13. Shortage/Shrinkage Metric
6. Officer Performance Metric Panel	14. Phone Theft Metric
7. Security-Safety Metric	15. Security Inspection Findings Metric
8. Security Incidents Metric	16. Infringing Website Compliance Metric

The metrics come from a variety of industries and locations:

Sources of Metrics	
Industries	Locations
Defense/aerospace Energy/oil Finance/banking Government Insurance Manufacturing/industrial products Pharmaceutical Real estate management Retail Security services Shipping/logistics Telecom	United States Africa Australia/Asia Pacific Europe

The metrics are not presented as models of perfection. Rather, they are authentic examples that security professionals can follow, refine, or otherwise adapt when developing their own metrics.

A. Environmental Risk Metric

At a major insurance company headquartered in the Midwestern United States, the assistant vice president for corporate security uses an environmental risk metric to help the company decide where to place office facilities around the country. The metric, in use for 12 years, is designed to serve the risk management needs of the corporation.

The company owns or leases hundreds of facilities across the United States. Corporate security regularly collects a suite of data, assigns weights to various factors, and develops a numeric score that places each facility into a low, medium, or high category of risk. For each risk category, written policy specifies a collection of security measures that should be in place at the site. Exceptions can be granted, but the systematic approach results in uniformity and in efficiency in decision-making and security systems contracting. Most important, the *metrics-based approach helps senior management understand the level of risk in site selection and make informed decisions on risk management. In addition, over time, the metrics have steered the corporation toward having a smaller percentage of its locations in high-risk sites.*

The formula for the ongoing risk assessment metric creates a score from four elements:

1. CAP Index Score (local risk analysis) [CAP Index is a commercial provider of crime risk forecasting. CAP stands for Crimes Against Persons and Crimes Against Property.]

EFFECTIVE, EVALUATED SECURITY METRICS—© ASIS Foundation 2014

The average national crime rating score through CAP is 100. CAP is valued as follows: 1 – CAP score of 100 or lower; 2 – CAP score of 101 to 200; 3 – CAP score of 201 to 300; 4 – CAP score of 301 to 400; 5 – CAP score of 401 to 500; 6 – CAP score of 501 to 600.

Locations with a score of 601 or more will not be considered as a location for an office.

2. Type of environment

1 – Non-critical: storage, empty space, surplus equipment. Locations that, if rendered inoperable, would have little or no negative impact on business processes. 3 – Sensitive: administrative, claims, trial office, sales office or other public contact. Locations that, if rendered inoperable, could have their work transferred to another location with little impact to the business. 5 – Mission critical: IT/data center, call center, headquarters. Locations that, if rendered inoperable, would negatively impact the business for an extended period.

3. Sensitivity of the asset

1 – Low: Nothing of irreplaceable value including non-identifying records, furniture, low value equipment, perishable supplies, surplus assets. Facility may not be identified/branded as a corporate asset. 3 – Medium: Valuable equipment, associates, personally identifying records. Facility is branded as a corporate asset. 5 - High: Critical information/data, leadership associates, board members, cash/cash equivalents and critical infrastructure. Facility is identified as an integral part of the corporation, branded and well known in the community.

4. Occupancy type

1 – Unoccupied space; 2 – Mixed tenant space; 3 – Sole tenant

The risk levels are then defined by totaling the preceding scores: Low-risk location = 4 to 9 points; Medium-risk location = 10 to 15 points; High-risk location = 16 to 19 points.

The metric is presented quarterly to the corporate risk committee, and corporate policy defines the security measures required at each level of risk.

Most of the data is objective, and data collection is timely. The initial design of the data collection system for this metric required a significant amount of administrative time, but the ongoing cost is minimal.

This metric demonstrates a return on security investment in two ways. First, through the standardization that the policy calls for, the company can obtain long-term national contracts at favorable prices (e.g., alarm monitoring). Second, company surveys show that employees feel safe in corporate facilities and can work better when they feel safe. Thus, the metric, which increases site safety, measurably improves employee morale and productivity.

The metric helps senior management place facility site risk in perspective. Over time, it steers site selection toward safer areas. The metric also provides uniformity in specifying site security measures.

This metric puts security efforts into a language—the language of risk—that the insurance company's senior managers readily understand. The following graphic is an example of what the metric user presents to senior management:

Enterprise Physical Security Risk Dashboard

Enterprise Physical Security Risk Dashboard

YTD Critical Events

➤ XYZ location officers saved an associate's life during a heart attack. Officers across the company intervened in 12 assaults to save people from serious harm.

➤ An armed assailant led police through the downtown district only to be captured with the assistance of our officers.

➤ 13 high risk threats to the workplace and/or our associates were successfully de-escalated by the IMT.

➤ Security officers extinguished 12 fires.

	Laptop Theft	Assault	Threats
Overview	Laptops are the most stolen item across company. These thefts are primarily due to unsecured devices left in associate cars	The areas around our largest campuses have seen a slow increase in the number of assaults on the public who may be visiting these areas	Threats can come from claimants, policy holders, associates, and family members. Threats are directed against our facilities, associates, and agents
Sources	External	External	Both internal and external
Trend	Continues on pace with previous years	After a low in 2011 we have seen increases in 2012 and 2013.	After an exceptionally light year in 2012 threats have quadrupled in number. Significant assets are used to investigate and mitigate these threats

CAP Score (Crime Risk)
Distribution Across All Sites

Site Count (y-axis: 0, 10, 20, 30, 40, 50, 60, 70)

CAPS Score Ranges (x-axis: 0-100, 101-200, 201-300, 301-400, 401-500, 501-600, 601-700, 701-800, 801-900, 901-1000, 1001-1100)

CAP Risk Distribution Vs. Industry

Legend: ■ Low ■ Medium ■ High

(y-axis: 0%, 10%, 20%, 30%, 40%, 50%, 60%, 70%, 80%, 90%, 100%)

(x-axis: Industry, Us)

Expert reviewers (three rather than the usual two) and a member of the research team gave the metric the following scores, using the Security MET:

Metric 3	Researcher	Expert 1	Expert 2	Expert 3	
Criterion	Score	Score	Score	Score	Average
1. Reliability	4	3	4	5	4.00
2. Validity	4	3	4	5	4.00
3. Generalizability	3	4	4	5	4.00
Technical Total	**11**	**10**	**12**	**15**	**12.00**
4. Cost	3	5	5	3	4.00
5. Timeliness	5	5	5	5	5.00
6. Manipulation	4	4	4	5	4.25
Operational (Security) Total	**12**	**14**	**14**	**13**	**13.25**
7. Return on Security Investment	5	2	3	5	3.75
8. Organizational Relevance	5	5	5	5	5.00
9. Communication	5	4	4	5	4.50
Strategic (Corporate) Total	**15**	**11**	**12**	**15**	**13.25**
TOTAL ACROSS CRITERIA	**38**	**35**	**38**	**43**	**38.50**

The expert reviewers made the following observations:

> This is a useful tool for determining the risk associated with various sites and determining what security controls should be in place at each location. Ongoing review of CAP scores provides continuous evaluation. It might be beneficial to add other data sources to the metric, as well. The metric is straightforward, easy to maintain, and fairly easy to understand. Tying it to organizational policy increases the likelihood of consistent implementation of security measures.

> One could also attempt to measure or calculate the cost of security measures that would be needed to lower a site's risk score. Another metric could examine losses and incidents at a site both before and after implementation of countermeasures.

B. Personnel Security Clearance Processing Metric

At a defense contractor headquartered on the east coast of the United States, personnel security clearance processing is a vital step in the hiring process. The company hires about 2,500 new personnel per year, but because of the length and unpredictability of the clearance process, it generally was not possible to give candidates firm starting dates. Offering contingent start dates made the company lose good candidates to firms that offered firm starting dates. Moreover, each day of waiting for clearance processing was a day that the candidate could not be employed on, and billed to, a project.

By examining the clearance process, step by step, from an enterprise point of view, security was able to:

- cut the cycle time by 50 percent (through prescreening and process improvement), getting people to work faster

- develop a tool that tells hiring managers what start date they should offer to a candidate, strengthening the recruiting position

- save significant sums in payroll paid before employees are billable

The metric measures the following:

- end-to-end performance (from posting a position requirement to having a billable employee)

- cost (e.g., cost by security service offering, return on investment, investment vs. performance, increased productivity/revenue generation)

- risk reduction (potential clearance delays; reduction of contingent hires; reduction of error rates; reduction of packages rejected because they need additional information)

- savings (reduction in the cost of bad hires; reduction in processing staff/footprint; reduction in overhead/sitting on the bench before clearance approval)

Designing this metric was expensive ($3 million), but security successfully presented the business case and received significant funding. The data is provided in real time, is system-generated, and has complete audit trails.

The metric has been useful for demonstrating the following returns on security investment:

- 40 percent reduction in personnel security clearance processing staff/footprint

- 50 percent reduction in personnel security clearance cycle time, equating to more than $30 million in increased productivity and revenue

- savings to the enterprise by hiring best-in-class candidates (reducing clearance delays) and avoiding the loss of candidates to other organizations

The clearance processing project is clearly aligned with the organization's goals. For example:

- 80 percent of corporate revenue comes from cleared staff, so getting them to work faster increases revenue.

- people are the company's number one asset, so a metric that leads to better hiring benefits the enterprise.

- personnel security is considered one of the top 10 risks to the enterprise.

The metric is easy to explain to senior management, as nearly everything in it equates to costs, revenue, and risk reduction. The metric helps security demonstrate the results of its work to executive staff and gain support for continued funding for security innovations and enhancements.

EFFECTIVE, EVALUATED SECURITY METRICS—© ASIS Foundation 2014

Expert reviewers and a member of the research team gave the metric the following scores, using the Security MET:

Metric 9	Researcher	Expert 1	Expert 2	
Criterion	Score	Score	Score	Average
1. Reliability	5	5	5	5.00
2. Validity	5	5	5	5.00
3. Generalizability	4	5	4	4.33
Technical Total	**14**	**15**	**14**	**14.33**
4. Cost	1	3	2	2.00
5. Timeliness	5	5	5	5.00
6. Manipulation	5	5	5	5.00
Operational (Security) Total	**11**	**13**	**12**	**12.00**
7. Return on Security Investment	5	5	5	5.00
8. Organizational Relevance	5	5	5	5.00
9. Communication	5	5	5	5.00
Strategic (Corporate) Total	**15**	**15**	**15**	**15.00**
TOTAL ACROSS CRITERIA	**40**	**43**	**41**	**41.33**

The expert reviewers made the following observations:

> Staff understood how gaps in their program were creating unnecessary expenses. They examined their processes and developed a four-part metric that scores well on the Security MET. The cost of creating an automated, dashboard-driven data collection tool was high, but the benefit was shown to be higher. This metric is easy to understand and shows the benefits of security initiatives. It could also be useful at some point to measure personnel quality.

C. Phone Theft Metric

At a major financial services firm in the Midwestern United States, the vice president for security developed a metric that tracks assaults. Specifically, it tracks assaults on employees who work at the company's offices in the city's central business district. The metric is part of the company's risk management effort and its effort to attract and retain workers.

The metric focuses on "Apple picking," which is the theft of mobile phones by criminals who grab the phones out of users' hands. At the company's downtown office sites, a severe rash of phone theft developed. Employees were victimized on the sidewalks all around the offices—as they came to work, when they went outside for lunch, and when they left to go home.

Matters escalated to the point where employees experienced 40 phone thefts in two months. Security's incident tracking process showed how many thefts occurred, where they occurred exactly,

and when. With that data, it was possible to identify hot spots and times for phone theft and apply extra security measures at those places and times. The company:

- installed more cameras in the hot spots.

- placed security officers outside the buildings instead of in the lobbies at the morning rush, lunchtime, and evening rush.

- asked for and received increased police patrol at the hot spots (the request being supported by the company's incident reports and video images).

- directed its security officers to approach employees who looked vulnerable (not paying attention while talking on phones) and hand them special flyers with information on safe behavior and phone retrieval/locator apps.

- created "be on the lookout" sheets and sent them to 30 local security directors and all company parking attendants.

- in concert with the local police, investigated the thefts, and some of the thieves were subsequently caught.

After the company took these measures, phone theft was eliminated. After a height of 40 thefts in two months, the number is now down to zero.

The metric—the number of mobile phone thefts—is highly reliable, as it is based on incident reports from victims (employees), police reports, and video surveillance. Likewise, the metric's utility appears to be confirmed by the outcome: the company had reliable reports of theft, it took security action based on those reports, and now the problem is eliminated. Collecting the data presents little marginal cost, as the company already tracks and trends security incidents using incident management software.

The vice president for security noted that the company values the metric. It is perfectly aligned with the company's goal of attracting, protecting, and retaining talent at its office locations in a city that experiences a high rate of crime. The company's risk management department pays close attention to this metric and related metrics. However, it is hard to quantify the value of keeping employees safe and continuing to attract new employees.

The vice president for security reports this metric and related data to senior management every quarter to show the value of the security program. The following are some graphics used recently:

EFFECTIVE, EVALUATED SECURITY METRICS—© ASIS Foundation 2014
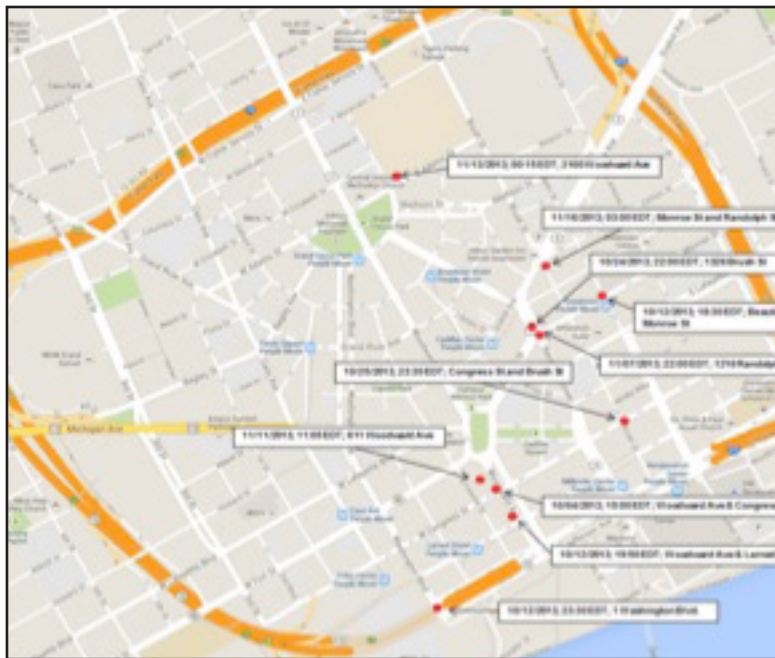
Third Quarter 2013

Fourth Quarter 2013 (theft reduced)

Expert reviewers and a member of the research team gave the metric the following scores, using the Security MET:

Metric 14	Researcher	Expert 1	Expert 2	
Criterion	Score	Score	Score	Average
1. Reliability	5	4	5	4.67
2. Validity	4	4	5	4.33
3. Generalizability	4	2	5	3.67
Technical Total	**13**	**10**	**15**	**12.67**
4. Cost	4	4	5	4.33
5. Timeliness	4	4	4	4.00
6. Manipulation	4	3	4	3.67
Operational (Security) Total	**12**	**11**	**13**	**12.00**
7. Return on Security Investment	2	4	5	3.67
8. Organizational Relevance	5	4	5	4.67
9. Communication	5	5	5	5.00
Strategic (Corporate) Total	**12**	**13**	**15**	**13.34**
TOTAL ACROSS CRITERIA	**37**	**34**	**43**	**38.00**

The expert reviewers made the following observations:

This metric served a useful purpose in quantifying a problematic threat and vulnerability and tracking the positive impacts that a multifaceted security countermeasure strategy had over time. The simplicity, reliability, and validity of the data led to readily understandable reporting to corporate leadership and a straightforward justification for additional security resources (where return on investment could clearly be seen). This example shows that a metric may be used for a short period and can be phased out once a specific problem has dissipated.

VII. Presenting Metrics to Senior Management

A key task in this research was to develop guidelines for effectively using security metrics to persuade senior management.

As this project's literature review notes:

> Corporate management tends to view security as overhead (i.e., a cost center rather than a production center) and security metrics as merely measuring activity, not value. Security professionals note that security benefits are difficult to measure compared to the benefits of profit centers, and such professionals often lack the skills or time to create and administer effective metrics. Thus, current security metrics, in practice, are generally not compelling and are often not taken seriously (Rothke, 2009).

This project's online survey found that 80 percent of respondents who use metrics share their metrics outside the security department. Of those who share, 79 percent share with senior management. That means about 56 percent of survey respondents who use metrics share those metrics with senior management.

What would make those presentations more compelling? This section presents advice gathered from a variety of sources: the literature review, the online survey, the follow-up telephone interviews, the advisory board, and the expert panel. Several key recommendations emerge from those sources:

- Present metrics that are aligned with the organization's objectives or risks or that measure the specific issues management is most interested in.
- Present metrics that meet measurement standards.
- Tell a story.
- Use graphics, and keep presentations short.
- Present metric data regularly.

A. Align with Organizational Objectives and Risks

As this project's literature review observes:

> Before choosing a metric, security professionals should identify the data that is most important to senior management; metrics should be selected and communicated in accordance with the data that is of most importance to the audience (Pironti, 2007).

Experts advising the researchers emphasized the importance of focusing metrics on organizational risks and objectives, as well as any other issues that are important to senior executives. Moreover, 70 percent of online survey respondents said their metrics are aligned with the organization's risk process or objectives. One respondent explained how his metrics are aligned with organizational objectives:

> The metrics partly demonstrate how objectives are being met. The objectives are set top down. Therefore, the security performance directly affects the performance of the C-suite member responsible.

In addition to aligning metrics with the organization's overall objectives, the security professional should focus metrics on risk and return on investment (ROI).

1. Risk

Survey respondents and interviewees offered several insights regarding the use of security metrics to address an organization's risk:

- We are part of the organization's integrated risk management process.

- We mainly use the metric to show business heads that we are not slowing them down. The metric shows that we are protecting the company from unsuitable business partners while keeping to an announced, short cycle time in our due-diligence investigations.

- The metrics-based approach helps senior management understand the level of risk in site selection and make informed decisions on risk management. In addition, over time, the metrics have steered the corporation toward having a smaller percentage of its locations in high-risk sites…. One of my goals is to help the organization decide on its security risk appetite. I try to get senior leadership to pay attention and help decide how much risk to accept…. We're an insurance company…. This metric puts our security work into a language—risk—that senior management can understand.

- Our metric helps senior management properly estimate the risk associated with various ways of conducting business. For example, our ongoing metric regarding losses averted from several types of fraud…helps senior management develop corporate strategy, in particular by helping to quantify the risks associated with e-commerce.

2. ROI

The literature review notes:

> Return on investment (ROI) is a widely known construct that can be applied to ensure effective metric communication. ROI can be a vehicle for metrics to justify budgets and can help in examining financial inputs and outputs of various security activities; these factors are of utmost importance to management and key stakeholders (Martin, Bulkan, & Klempt, 2011; Hastings, 2013). Unfortunately, calculating ROI is not straightforward, particularly in the security realm (Thompson, 2010). However, when available, ROI data can be a great tool to harness management attention and action.

Interviewees (those who shared details for the metric summaries in this report) offer the following insights into how they use metrics to show a return on the organization's security investment:

- We were performing security audits four times per year, but analysis of our findings suggested we could cut the audits back to three times per year. Further analysis of the audit metrics over time showed that security weaknesses ("findings") did not increase. Thus, we reduced costs and administrative burdens and did not increase risk to the corporation…. Most likely, a much larger return on investment comes from our reduction of the likelihood of external and internal failures. However, that ROI is harder to quantify.

- Our metric—office space usage—is extremely valuable to senior management. We track the actual savings from renegotiated contracts for space leases. The metric provides a clear economic benefit.

- With our security activity metrics, it is common for us to determine that because little activity takes place at a site, we can reduce or eliminate uniformed security officers there. That is a quantifiable return on investment. We also use our metric to support requests for security expenditures.

- Senior management's basic question to us is this: Considering the entire program and all expenses, does the assets protection function accomplish anything that can be quantified and that justifies the allocation of the funds expended? Our metric directly answers this question. The most important use is to prove to the CEO and to the chairman that it is possible to pilot security like all other the processes in the company and obtain a return on investment—to employ security in line with the company's overall financial approach.

- There is a clear link between reducing shrinkage and saving money. Our metrics demonstrate that investment in security technology led to reduced losses. We have found that if shortage goes up, senior management is willing to allocate resources to help us determine the cause and implement solutions.

If a metric relates to risk, return on investment, or overall organizational objectives and management interests, the metric is more likely to be compelling to senior management than a metric that merely collects security-related data without putting it in a management context.

The following box shows how one security professional proposes to calculate return on investment in terms that his company's financial executives understand:

ROI Metric

A security executive shared the following:

It would be nice to have a financial metric that speaks the language of our finance leaders—something that could be easily recognized and supported by hard data.

Consider this equation:

Capital Investment (CI) X Cost of Capital (CC) = Target

CI X CC = T

Capital Investment: my operating budget—say, $10 million

Cost of Capital: How much the company could expect to make on the security investment if the company put that money in the market. The cost of capital is determined by a company's chief financial officer. In this case it is 5 percent.

Target: the amount of savings I need to produce to provide a return on investment

$10 million X .05 = $500,000

Most of what we do is based on the cost of what doesn't happen. Our actuaries are researching the average number of FBI Index crimes per capita and what each may cost the organization. We will then show if we are above or below the average and, if below, what those savings or avoided costs are. We hope that total will be more than the target ROI above and thus prove value. This figure will be in a language our industry understands because we use actuarial data regularly.

Jay C. Beighley, CPP, CFE
AVP, Corporate Security
Nationwide Corporate Security

B. Present Metrics That Meet Measurement Standards

As the literature review notes:

> Grounding metrics in the principles of measurement is crucial in capitalizing on the benefits of metrics (Dix, 2013).

Because metrics are quantitative, they exude a scientific authority. However, if a metric is based on invalid or unreliable data, one cannot draw accurate conclusions from it and it will lack external credibility. A metric that has been properly designed from a scientific point of view and that has been evaluated against a testing tool (such as the Security MET) may appear more valuable and persuasive to senior management.

Using a metric that meets measurement standards also provides an objectivity that aids decision-making. As one interviewee noted:

> Primarily it helps us resolve conflicts without pointing fingers at individuals. We are able to define through metrics when a process or procedure has not achieved the desired result and make the necessary corrections rather than just point a finger at an individual and say "shame on you," which does not correct the problem. Metrics make it about the process or procedure rather than personality.

C. Tell a Story

As the literature review observes:

> Communicating metric value remains a challenge. It does not matter how great the data is if it cannot be understood by key stakeholders (Dix, 2013).... One can be more persuasive by using metrics to tell a story—that is, by collecting metrics that are forward-looking and backward-looking and by addressing the questions "Where are we going?" and "Where have we been?" (Campbell, 2011; Blades, 2012). Security professionals can best explain their findings by providing specific, concrete examples that are meaningful to the audience (Deming, 2012).

The metrics-based story that a security professional tells to senior management can be told as a story about risk—the specific risk that security is attempting to mitigate, as well as the consequences if the event occurs. To make the story compelling, security professionals should name the actual business resources threatened and the value of those resources. It is best to be straightforward about risk and uncertainties; evasiveness may lead to perceptions of dishonesty.

Part of a compelling story is the unfolding of events over time. Metrics can show progress toward the meeting of a specific strategic goal. Incident management software may help make organizing and discerning meaning from data (i.e., trends analysis) faster and less burdensome.

Benchmarking, too, can enrich a story, as long as it is aligned with strategic organizational goals. Benchmarking grants organizations the opportunity to ascertain where they stand on a given metric in relation to their competitors. However, benchmarking depends on organizations' willingness to share their data, which they often decline to do.

D. Use Graphics, and Keep Presentations Short

The effectiveness of a metrics presentation has to do not only with content but also with presentation style. This project's advisors and interviewees provided several recommendations for persuasively presenting metrics in a clear, concise manner that serves management's needs:

- As vice president for security, I report this metric to senior management every quarter to show the value of the security program. I present the data in summary form in a PowerPoint presentation. The key is to keep it simple and clear. Present a few short bullet points—top-level information only, rather than complex charts and graphs. A dashboard containing multiple charts and graphs may be useful internally (within a security department), but for presentations to senior management, simpler is better.

- Our metric is easy to explain to senior management. Over time, we have learned that less is more. We asked senior management what they really wanted to see. They said they cared about only seven particular items from our 30-page report. Now we give a short slide presentation about our metrics—no more than 10 slides. I am working to create an even simpler dashboard for senior management.

- We provide a dashboard of only the most important security metrics. We limit our presentation to 5 minutes.

- We use the analytics and graphing features included in our incident management software.

- Use graphics, but not too many. Keep it simple, and remember that less is more. We first determine what is significant. Different leaders like different presentations. We summarize our findings and do not bother executives with trivial information. "Risk charts" (see illustration below) resonate with senior management. We show the probability and severity of potential events and then present our risk mitigation strategy.

The following boxes present graphics supplied by interviewees for the project's metric summaries.

CAP Score (Crime Risk) Distribution Across All Sites

CAPS Score Ranges

CAP Risk Distribution Vs. Industry

- Low
- Medium
- High

Industry   Us

Averted Losses

Guest Check-out filters have helped increase averted losses. New automated fraud solution implemented in 2013 with goal of 50% fraud reduction.
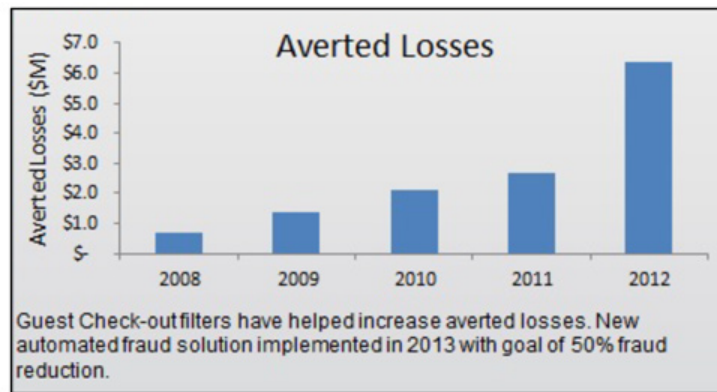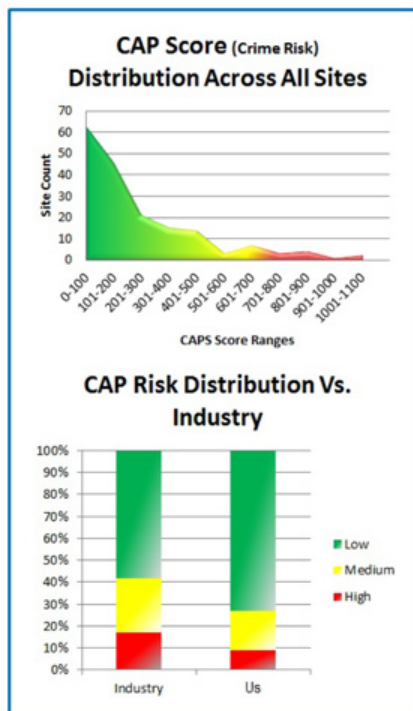
Sample Graphics in Use in the Field

Top left: Graphs show the company's facilities are mostly in low-crime districts and are more heavily weighted toward safe locations than are its competitors' facilities.

Top right: Graph shows significant increase in losses averted.

Bottom: For presentations to senior executives, security managers place various risks into the correct boxes to show the likelihood and severity of occurrence.

Likelihood of Occurrence:
- Near Certain 5 — L>90%
- Highly Likely 4 — 70<L<90%
- Likely 3 — 30<L<70%
- Low 2 — 10<L<30%
- Not Likely 1 — L<10%

Severity of Occurrence:
- Minimal 1
- Minor 2
- Moderate 3
- Major 4
- Severe 5

Will result in a Serious DSS finding if proper action not taken

Will result in a Repeat Systemic DSS finding if proper action not taken

Will result in an Administrative DSS finding if proper action not taken
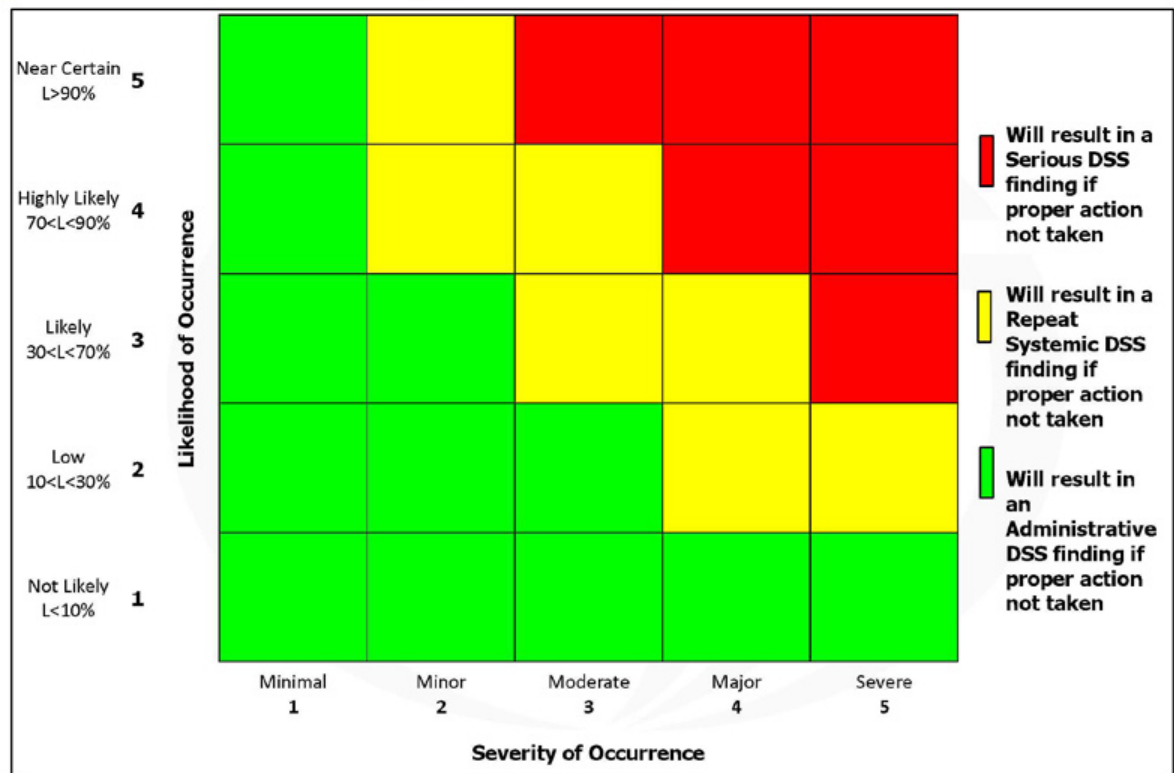
Employee phone thefts, third quarter 2013
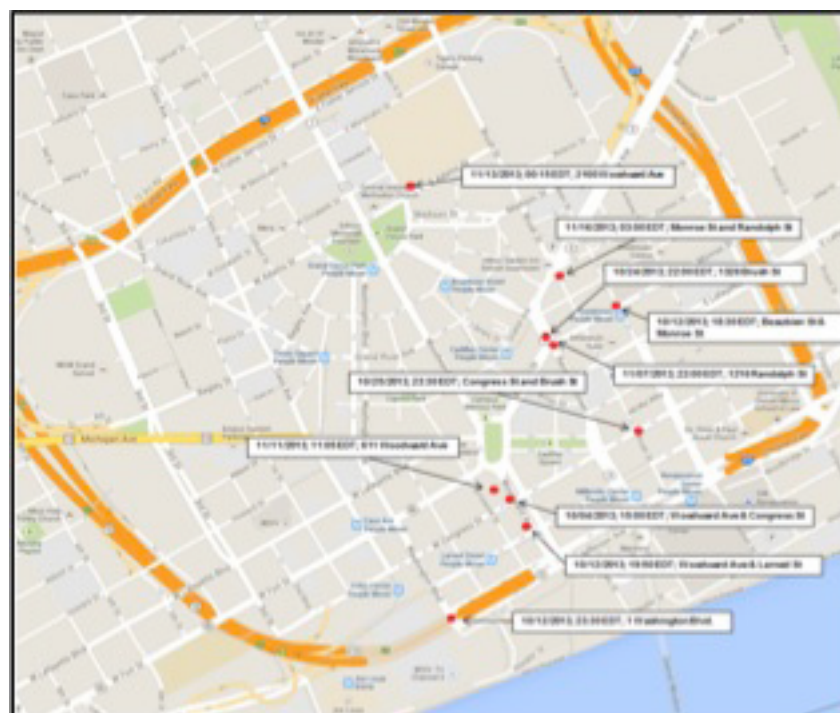
Employee phone thefts, fourth quarter 2013 (theft reduced)
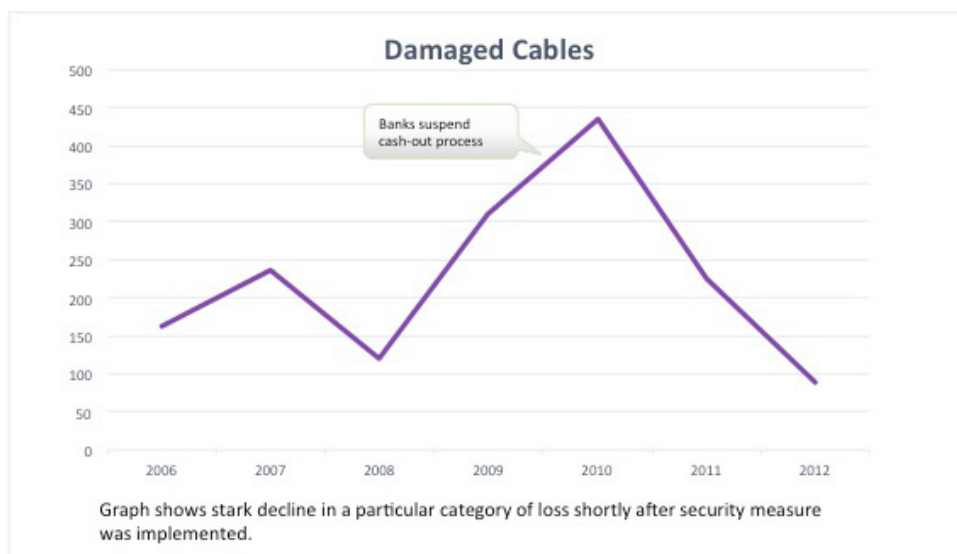
Damaged Cables

Graph shows stark decline in a particular category of loss shortly after security measure implemented.

E. Present Metric Data Regularly

Survey respondents reported sharing their metrics with senior management at different intervals. Among those who share their metrics outside the security department, 40 percent do so monthly, 43 percent quarterly, and 17 percent annually.

The research does not suggest an optimal interval for sharing security metrics with senior management. However, combining the preceding figures, the survey shows that 83 percent of security professionals who share metrics outside the department do so at least quarterly. As data ages, it could become more historical, less actionable, and thus potentially less valuable. Distinguishing metrics that are time-sensitive from those that provide value over time will enhance the overall value of metrics.

VIII. Future Practitioner Needs

Through a literature review, online survey, telephone survey, and guidance from an advisory board and expert panel, this research has attempted to increase the body of knowledge about the use of metrics in security. It has also produced the following:

- **Security Metrics Evaluation Tool.** This is a 15-page, self-administered tool for evaluating a metric against nine criteria, divided into technical, operational, and strategic categories. It is designed to point out a metric's strong and weak points so that weaknesses can be corrected.

- **Database of selected security metrics.** The report contains 16 metric summaries, each evaluated by three reviewers according to the Security MET criteria. The metrics measure a wide variety of issues and come from a wide variety of industries (as well as several different countries). Some of the metrics are more sophisticated than others, providing a range of examples for potential users to study. The metrics are not presented as models of perfection. Rather, they are authentic examples that security professionals can follow, refine, or otherwise adapt when developing their own metrics.

- **Guidelines for effective use of security metrics to persuade senior management.** The report presents guidelines gathered from the literature review, the online survey, the telephone interviews, the advisory board, and the expert panel. Recommendations include presenting metrics that are aligned with the organization's objectives or risks or that measure the specific issues management is most interested in; presenting metrics that meet measurement standards; telling a story; using graphics; keeping presentations short; and presenting metric data regularly.

Future possible needs in the field include the following:

- **Larger metrics library.** This report presents 16 metric summaries, evaluated by experts and researchers. It would be useful to discover, summarize, and evaluate more metrics and build a larger library that practitioners can consult. A larger library might also facilitate benchmarking.

- **Metrics training for security practitioners.** This could take the form of a video, a webinar, interactive online training, or an instructor-led module in a workshop or seminar. The training could teach security professionals how to use the Security MET, the database of metric summaries, and the guidelines for persuasive metric presentations. Successfully developed metrics could be included in a growing metrics library.

- **Follow-up contact with metric survey respondents who indicated they would like more information about metrics.**

- **Tool for creating a metric from scratch and implementing it in an organization.** The present research focused on helping security professionals discover existing metrics, evaluate them in order to improve and adapt them, and present them to senior management effectively. Another research project could take a different approach, attempting to develop a detailed yet simple fill-in-the-blanks template that practitioners could use to develop and implement a metric from scratch. A further possibility is to design a software application to create, collect, and store metrics using a dashboard model.

- **Audited metrics.** The current metric summaries are based on descriptions provided by the metric users. A deeper level of research would obtain the fine details of a metric and subject it to outside audit. That approach could lead to a highly detailed account of a metric's creation, use, and effects in a particular setting.

- **Additional publications.** To spread the project's findings further, it could be useful to develop other publications from the research, such as magazine articles, journal articles, or handbooks.

- **Certification.** ASIS could consider developing a security metrics certification, along with metrics training. The subject of metrics could also be emphasized in Certified Protection Professional training and testing.

- **Metrics standard.** ASIS has produced numerous standards so far and could create a new standard on metrics development and use.

Appendix A: Security Metrics Evaluation Tool (Security MET)

A particular security metric may seem worthwhile. Collecting data for it may be simple and quick, and the metric itself may be easy to explain to senior management. The metric may also have serious flaws. Perhaps the data is scientifically unreliable or is easy to manipulate, or the metric has little connection to the organization's strategic mission or risk management concerns—in other words, the factors that matter most to senior management. To use a security metric most effectively, security professionals need an organized way to examine it across relevant criteria so that weaknesses in the metric can be corrected.

This Security Metrics Evaluation Tool (Security MET) is intended to help security professionals assess the quality of a given metric. It is a framework for discerning the strong and weak points of a security metric, based on criteria that matter to senior management. A metric that scores high on the Security MET would have a high degree of technical value (scientific merit), operational reasonableness (considering cost and time), and strategic relevance (link to organizational risks or goals). It would also be persuasive when presented to senior management.

You will rate your metric based on nine criteria. The criteria are grouped in three categories:

Technical Criteria – Category 1

    1. Reliability

    2. Validity

    3. Generalizability

Operational (Security) Criteria – Category 2

    4. Cost

    5. Timeliness

    6. Manipulation

Strategic (Corporate) Criteria – Category 3

    7. Return on Investment

    8. Organizational Relevance

    9. Communication

Each criterion is explicitly defined. For each criterion, you will assign the metric a score of 1 to 5 with defined anchors for scores of 1, 3, and 5. Choose a score of 2 or 4 if the correct answer lies between the anchors. Examples after each criterion show how scoring might be applied.

A score sheet is presented at the end to tabulate the metric's score across the nine criteria.

Lower scores on particular criteria show where a metric has room for improvement. Total scores may be useful for comparing one metric to another.

Criterion 1: Reliability

Degree to which the metric yields consistent scores that are unaffected by sources of measurement error (e.g., the time when the measure was taken, the identity of the raters, the weather that day).

Illustration of the concept:

> *Construct or focus of metric: Product weight.*

> *Description of metric: Weight as measured with a postal scale.*

If a product is placed on a postal scale repeatedly (and at different times of day, by different persons), and each time the scale shows the same weight, the measure is highly reliable. In contrast, if the scale values change each time, the measure is unreliable.

Please rate the metric on the following scale. Read the description of each level and select the number that most closely corresponds to the metric. Mark the score on the score sheet at the end of this tool.

1 = low reliability, 5 = high reliability

Data for this metric is not collected very carefully; repeated measurements by the same method reach different figures; different methods of measuring reach different counts when they should reach the same counts; there is over- or under-counting; the user has low confidence in the data.		Data for this metric is collected fairly carefully; repeated measurements by the same method usually reach the same figures; alternate counting methods usually reach the same figures; there may be some over- or under-counting; yet the totals are plausible.		Data for this metric is collected very carefully; alternate counting methods reach the same figures; repeated measurements by the same method reach the same figures; there is no over- or under-counting; overall there is a high likelihood that the metric is reliable.
1	2	3	4	5

Metric: Annual voluntary turnover of employees in a security department.

> **Example Score:** Human resources staff easily calculate this metric. This measure is straightforward and could be consistently applied over time, by different people. It is highly unlikely that any errors would be made. As a result, this metric would receive a 4 or 5 on this criterion.

Metric: Percentage of company employees who are the subject of current internal investigations.

> **Example Score:** In a large, multisite corporation, some local security branches keep poor records, supply their data late or incompletely, or interpret the data request incorrectly. The metric user cannot be sure all current investigations are being reported and that closed investigations are not counted. Also, it may be difficult to obtain a reliable count of current employees due to poor reporting from corporate branches. As a result, in this setting, the metric might receive a 2 on this criterion.

Criterion 2: Validity

Degree to which evidence based on theory or quantitative research (conducted by the user or others) supports drawing conclusions from the metric.

Illustration of the concept:

> *Construct or focus of the metric: Usefulness in retrieving items from high shelves.*

> *Description of metric: Height of the stool in inches.*

> *Evidence of validity might be provided by a theory that if people were able to reach higher shelves using taller stools, then using taller stools would also allow people to more effectively retrieve items from high shelves. Alternatively, empirical research might demonstrate that when people use taller stools, they are more effective at retrieving items than when they use shorter stools.*

Please rate the metric on the following scale. Read the description of each level and select the number that most closely corresponds to the metric. Mark the score on the score sheet at the end of this tool.

1 = little validation evidence, 5 = much validation evidence

The metric has only a **weak relation** to the problem it is trying to measure; there is **little or no evidence** that the metric can be used to draw conclusions; the user has **not tested** the metric to see whether decisions based on it are accurate.		The user has **anecdotal evidence** that the metric is a valid measure; the metric appears, **on its face**, to be measuring what matters; **non-research literature** (e.g., a trade publication) suggests that the metric is valid.		**Research literature** suggests the measure is **valid**; the **user** has **formally studied** the connection between the metric and the security concern for which it is being collected, and has found the metric to be **valid**.
1	2	3	4	5

Sample Applications:

Metric: The number of nuisance (i.e., false) alarms per month at all company facilities as a measure of user compliance.

> **Example Score 1:** The number of nuisance alarms varies considerably, not based on poor employee practices, but based on more random factors, such as buildings being used more or less often than usual or temporary interferences from migrating animals. This would warrant a 1 on this scale.

> **Example Score 2:** The metric has been shown (in studies by the user) to change in predictable ways after the user makes changes based on the metric. For example, every time the security director holds a series of security alarm awareness sessions for employees, the number of false alarms drops for a few weeks; the number rises again after a few weeks until the security director conducts more employee training. This would warrant a 5 on this scale.

Criterion 3: Generalizability

Degree to which conclusions drawn from the metric are consistent and applicable across different settings, organizations, timeframes, or circumstances; extent to which metric results allow for external comparison across organizations.

Illustration of the concept:

> *If organizations were interested in the weight of the same manufactured object, this measurement could be easily obtained over time and could be used by any organization, and organizations would be willing to share these results; as a result, there would be high generalizability. In contrast, if organizations were interested in the weight of their own unique manufactured object, while this measurement could be easily obtained and used by all organizations, meaningful comparisons could not be made (as the products are different across organizations); as a result, there would be low generalizability. Similarly, if organizations were unwilling to share their measurements, even for the same type of object, generalizability would be low.*

Please rate the metric on the following scale. Read the description of each level and select the number that most closely corresponds to the metric. Mark the score on the score sheet at the end of this tool.

1 = low generalizability, 5 = high generalizability

The conclusions drawn from the metric are **not consistent** and **not applicable** across different settings, organizations, timeframes, and/or circumstances; organizations are **not willing** to share the data derived from this metric; comparisons to external organizations **cannot be made** based on this metric.		The conclusions drawn from the metric are **sometimes consistent** and **sometimes applicable** across different settings, organizations, timeframes, and/or circumstances; organizations are **sometimes willing** to share the data derived from this metric; comparisons to external organizations **can sometimes be made** based on this metric.		The conclusions drawn from the metric are **consistent** and **applicable** across different settings, organizations, timeframes, and/or circumstances; organizations are **willing** to share the data derived from this metric; comparisons to external organizations **can almost always** be made based on this metric.
1	2	3	4	5

Sample Applications:

Metric: Employee satisfaction surveys.

> **Example Score:** These surveys exist in some fashion in most large organizations. The exact questions vary, but the content of the questions is likely similar. It is somewhat likely that organizations would be willing to share this data with other organizations. For example, an organization might want to showcase how satisfied its employees are compared to employees in similar organizations. However, it is also possible that an organization might not share this data if its employees are dissatisfied. Based on these factors, this metric would receive a 3 on this criterion.

Metric: Annual voluntary turnover of employees in a security department.

> **Example Score:** Human resources personnel easily calculate this metric. This measure is straightforward and relevant to all organizations. It would be easy to compare the numbers derived from this metric. Most organizations are willing to share this data. As a result, this metric would receive a 5 on this criterion.

Criterion 4: Cost

Monetary and non-monetary costs associated with metric development and administration; also, negative consequences associated with the metric.

Illustration of the concept:

Construct or focus of metric: Product weight.

Description of metric: Weight as measured on a postal scale.

If a scale costs $50 to buy, can be used for 10 years by any employee, and the weighing process is quick and not disruptive to operations, then the metric has a low cost. In contrast, if a scale costs $500 per month to rent, requires extensive employee training, and works so slowly that operations are disrupted, then the metric has a high cost.

Please rate the metric on the following scale. Read the description of each level and select the number that most closely corresponds to the metric. Mark the score on the score sheet at the end of this tool.

1 = high cost, 5 = low cost

The cost of developing or administering the metric is **high**; **long** or **expensive** training of administrators is required; obtaining data places **severe** burdens on staff; collecting the data is **offensive** to employees or customers (intrusiveness, complexity, etc.); collecting the data puts proprietary or personal information **at risk**; the metric creates significant organizational **strife** or **disruption**; calculating the metric is **very** difficult.		The cost of developing or administering the metric is **moderate**; only **basic** training of administrators is required; obtaining data places only **moderate** burdens on staff; collecting the data creates at most a **minimal** risk of offending employees or customers or disrupting operations; calculating the metric requires a significant but **acceptable** level of effort; overall, there are **few** downsides to using the metric.		The cost of developing or administering the metric is **minimal**; **little** or no training of administrators is required; staff can obtain the data **quickly** and **easily**; collecting the data does **not** offend employees or customers or disrupt operations; calculating the metric is **quick** and **easy**; overall, there are **no** significant downsides to using the metric.
1	2	3	4	5

Sample Applications:

Metric: The number of door alarm annunciations per month.

> **Example Score:** This measure could be obtained instantly through an incident management system; this system might have a reporting capability where reports on the frequency of alarms can be calculated in minutes. The installation of the incident management system requires an initial fee of $5,000. A one-hour training is sufficient to train security personnel on the system's capabilities. As a result, this metric would receive a 4.

Metric: The number of attempted computer hacking incidents blocked per month.

> **Example Score:** Blocking attempts to hack the company's computers is valuable, but counting the blocked attempts is very difficult and time-consuming. It requires 20 hours of information technology staff time to determine how many attempts were stopped. The value of knowing exactly how many attempts were stopped is uncertain, and the cost of obtaining the information is high. In this instance, the costs associated with obtaining the metric are unjustifiably high; as a result, 1 or 2 would be an appropriate selection.

Criterion 5: Timeliness

Extent to which metric data can be gathered in a timely fashion so the results can have an impact.

Illustration of the concept:

> *If a person is interested in the weight of an object, a scale could be used to instantly capture this measurement; this would reflect high timeliness of data. However, if the item must be shipped to another location to be weighed accurately, and there is routinely a backlog of items to be weighed, there would be a low timeliness of data.*

Please rate the metric on the following scale. Read the description of each level and select the number that most closely corresponds to the metric. Mark the score on the score sheet at the end of this tool.

1 =low timeliness, 5 = high timeliness

The data for this metric is **out-of-date** by the time it can be gathered and interpreted; the data collection process is **very** time-consuming; the data is **unlikely** to have an impact (as it **does not** reflect current conditions).		The data for this metric is **fairly up-to-date** by the time it can be gathered and interpreted; the data collection process is **somewhat** time-consuming; the data is **somewhat likely** to have an impact (as it **somewhat** reflects current conditions).		The data for this metric is **very up-to-date** when gathered and interpreted; the data collection process is **not** time-consuming; the data is **very likely** to have an impact (as it **reflects** current conditions).
1	2	3	4	5

Sample Applications:

Metric: Laptop computer losses (theft, misplacement, etc.).

> **Example Score:** Reporting at one company may be slow, so that when the security manager looks at the numbers, they reflect laptop losses from six months ago. This data would be too out-of-date to draw conclusions or guide decisions regarding laptop losses. As a result, this metric would receive a score of 1 on this criterion.

Metric: Annual voluntary turnover of employees in a security department.

> **Example Score:** Human resources personnel easily calculate this metric. This measure is straightforward and could be quickly applied over time, by different people. It is highly unlikely that any calculations would be out-of-date; thus the data derived could be used for drawing conclusions and making decisions regarding annual voluntary turnover. As a result, this metric would receive a 5 on this criterion.

Criterion 6: Manipulation

Extent to which metric data cannot be coached, guessed, or faked by staff; extent to which metric has built-in data quality checks or oversight.

Illustration of the concept:

> *Construct or focus of metric: Product weight.*

> *Description of metric: Weight as measured with a postal scale.*

> *If the person weighing the product has no motivation to fake and is being video-recorded to ensure accuracy, this metric has a high resistance to manipulation. In contrast, if the person weighing has a high motivation to fake and is not being video-recorded, the metric has a low resistance to manipulation.*

Please rate the metric on the following scale. Read the description of each level and select the number that most closely corresponds to the metric. Mark the score on the score sheet at the end of this tool.

1 = high manipulation potential, 5 = low manipulation potential

The metric data is **quite** susceptible to **manipulation**; the persons providing the data likely have an **incentive** to manipulate it; there are **no** built-in data quality checks or oversight.		The data underlying this metric is **mostly** reliable, but the providers of the data **could alter** the data if they wanted; there is **little incentive** to manipulate the data; there are **minimally acceptable** built-in data quality checks or oversight.		The data underlying this metric **cannot** be tampered with; the data is generated by people with **no motive** for manipulating it; there are **built-in** data quality checks or oversight.
1	2	3	4	5

Sample Applications:

Metric: Number of laptop computer losses (theft, misplacement, etc.).

> **Example Score:** Laptop loss is hard to conceal and would have to be reported (because employees likely cannot work without a laptop). Data is likely to be correct. Human resources staff monitor reports and follow up with employees if the loss seems suspicious. This would receive a 4 on this scale.

Metric: Percentage of company employees who are the subject of current internal investigations.

> **Example Score:** In a large, multi-site corporation, security branches are required to record the percentage of company employees who are the subject of current internal investigations. This recording is done by entry-level security professionals who monitor the internal investigation paperwork. Only branches that have a percentage lower than 5 percent are eligible for annual bonuses. In addition, the entry-level professionals are not observed while working and no one is responsible for double-checking their tabulations. As a result, in this setting, the metric might receive a 1 on this criterion.

Criterion 7: Return on Investment

Extent to which metric can be used to demonstrate cost savings or loss prevention in relation to relevant security spending. This involves expressing the following in terms of dollars or some other unit relevant to decision makers: the cost of the security intervention, the effects of the security intervention, and any unintended consequences directly related to the intervention.

The following is one means of calculating return on investment:

$$ROI = \frac{\text{profit or gain (or losses avoided) due to security measures - cost of security}}{\text{cost of security}} \times 100$$

Illustration of the concept:

> *For example, if a person counted the number of car break-ins in the company parking lot and could clearly determine which security expenditures led to a reduction in break-ins, the metric would be strong at demonstrating return on investment. If the person could not determine which of many security measures affected the break-in rate, or what those measures cost, the metric would be poor for demonstrating return on security investment. A metric should receive a high rating on this scale if it is capable of clearly demonstrating ROI, even if the ROI itself is poor.*

Please rate the metric on the following scale. Read the description of each level and select the number that most closely corresponds to the metric. Mark the score on the score sheet at the end of this tool.

1 = low ability to show return on investment (ROI), 5 = high ability to show ROI

The causal relation between the security measure and the benefits gained is **not clear**; the cost of the security measure is **hard** to isolate; the benefits of the security measure are **hard** to calculate; the security action being measured has **negative** consequences that are significant but **not** measureable.	The metric **theoretically captures** the benefits of a security action in relation to the costs of the measure; however, it is **sometimes difficult** to measure the benefits, or it may **sometimes be difficult** to isolate the cost of the security actions.	The metric **very clearly** shows the relation between a security action, policy, or system and the benefits or returns it provides; **both** the benefits and the costs are **readily measureable**, not vague or theoretical; the relation between the security measure and the benefit gained is **clear** and **direct**.
1	2 3 4	5

Metric: The number of computer hacking incidents prevented each month through intrusion prevention software and management.

> **Example Score:** The software has a one-time cost of $10,000, and an information technology staffer must devote two hours per month to monitoring the system and viewing and counting flagged incidents. However, if this software was not implemented, a serious computer hacking incident could cost the company $50,000 and would require 40 hours of information technology staff time to repair the issue. In this instance, the benefits associated with software usage far outweigh the costs of the security measures (software and labor), and the metric is instrumental in demonstrating that return on investment. As a result, 4 or 5 would be an appropriate selection.

Metric: Average net cost per investigation per year (net = cost of investigation minus the value of any money or property recovered).

> **Example Score:** This metric should have a high correlation with return on investment. If the average investigation costs $2,000 and recovers $4,000 in money or property, the return on investment is clear, and the metric might receive a score of 5 on this criterion. By contrast, if investigations cost more than they recover, but there is reason to believe losses would grow much larger if they were rarely investigated, the metric might receive a lower score, such as a 2 or 3, because the metric fails to consider a key factor (deterrence) that would affect ROI. In that case, the metric may still have value according to other criteria, but its ability to demonstrate ROI would be poor.

Criterion 8: Organizational Relevance

Extent to which metric is linked to organizational risk management or a strategic mission, objective, goal, asset, threat, or vulnerability relevant to the organization—in other words, linked to the factors that matter most to senior management.

Illustration of the concept:

> *An organization has a goal of reducing the weight of the object it manufactures. If a scale is used to calculate the weight of manufactured products, this metric would be of high organizational relevance based on its linkage to the goal. In contrast, if a person measured the length of the object, the measurement would be of low organizational relevance.*

Please rate the metric on the following scale. Read the description of each level and select the number that most closely corresponds to the metric. Mark the score on the score sheet at the end of this tool.

1 = low organizational relevance, 5 = high organizational relevance

The metric is **not linked** to a specific organizational strategic mission, objective, goal, asset, risk, threat, or vulnerability; if linked, the linkage is **weak** and of **minimal relevance** to the organization; the data derived from this metric is of **little importance** to senior management.		The metric is **somewhat linked** to a specific organizational strategic mission, objective, goal, asset, risk, threat, or vulnerability; the linkage is **moderate** and of **some relevance** to the organization; the data derived from this metric is of **some importance** to senior management.		The metric is **explicitly linked** to a specific organizational strategic mission, objective, goal, asset, risk, threat, or vulnerability; the linkage is **strong** and of **high relevance** to the organization; the data derived from this metric is of **great importance** to senior management.
1	2	3	4	5

Sample Application:

Metric: Number of thwarted hacking attempts against company's cloud-based software.

> **Example Score:** A software company supplies a cloud-based application to its customers. A vital goal of the company is to keep the application properly functioning and available to clients 99.99 percent of the time. Therefore, a metric regarding the number of denial-of-service attacks thwarted through security efforts would be highly relevant to the organization's goals and would be of great interest to senior management. As a result, the metric would receive a 5 on this criterion.

EFFECTIVE, EVALUATED SECURITY METRICS—© ASIS Foundation 2014

Criterion 9: Communication

Extent to which the metric, metric results, and metric value can be communicated easily, succinctly, and quickly to key stakeholders, especially senior management.

Illustration of the concept:

If a metric is clear, simple, and succinct, and takes very little time to explain to senior management, it has high communicative ease. By contrast, if it is complex, obscure, and overly involved, and it takes a long time to explain to senior management, it has low communicative ease.

Please rate the metric on the following scale. Read the description of each level and select the number that most closely corresponds to the metric. Mark the score on the score sheet at the end of this tool.

1 = low communicative ease, 5 = high communicative ease

The metric and purpose of the metric are **difficult** to explain to key stakeholders (i.e., C-suite personnel, management, supervisors, subordinates, customers); it is **difficult** to explain the value the metric will add to the organization; the results of the metric and implications of the results are **difficult** to explain.		The metric and purpose of the metric are **somewhat easy** to explain to key stakeholders (i.e., C-suite personnel, management, supervisors, subordinates, customers); it is **somewhat easy** to explain the value the metric will add to the organization; the results of the metric and implications of the results are **somewhat easy** to explain.		The metric and purpose of the metric are **easy** to explain to key stakeholders (i.e., C-suite personnel, management, supervisors, subordinates, customers); it is **easy** to explain the value the metric will add to the organization; the results of the metric and implications of the results are **easy** to explain.
1	2	3	4	5

Sample Applications:

Metric: The number of viruses detected weekly in user files.

> **Example Score:** This metric and the purpose of this metric are easy to explain to key stakeholders. Also, the value and results of this metric are straightforward; as a measure of information and cyber security, this metric allows security professionals to gauge the security of their network and the effectiveness of their information protection systems. As a result, this metric would receive a 4 or 5 on this criterion.

Metric: The number of internal documents with improper sensitivity classification markings discovered each month.

> **Example Score:** This metric might be valuable within the security department, but when the user tries to explain it to senior management, he or she might have to first explain the internal classification system, then the marking rules, and then the possible implications of improper marking. At that point, the CEO might lose interest in the explanation; he or she may not even particularly care about the number of improperly marked sensitive documents. In this case, the metric might receive a 2.

Score Sheet

Criterion	Score
1. Reliability	
2. Validity	
3. Generalizability	
Technical Total	
4. Cost	
5. Timeliness	
6. Manipulation	
Operational (Security) Total	
7. Return on Security Investment	
8. Organizational Relevance	
9. Communication	
Strategic (Corporate) Total	
TOTAL ACROSS ALL NINE CRITERIA: Technical + Operational + Strategic	

The numbers on this score sheet, taken from the preceding pages, should provide insights into whether the evaluated metric is strong or weak when measured against specific criteria that matter. Low scores point out areas where a metric needs improvement. After making adjustments to the metric, the user might wish to administer the Security MET again and see if the score rises.

Every criterion is important. For example, a metric could receive high scores on eight of the nine criteria but still be fatally flawed if it scored a 1 on cost.

Scores on the Security MET criteria point out areas where a particular metric may need to be strengthened. The total score may suggest how close the metric is to attaining the highest possible score (45), but it is not likely to be useful for comparing different metrics, as the scoring would be different for users in different organizations.

Appendix B: Library of Evaluated Metrics

This section presents 16 summaries of metrics in use in the security field as of 2013. The summaries were developed primarily through telephone interviews. Participants were identified through this project's online survey, which asked respondents if they were currently using metrics and would be willing to describe their practices to a researcher. About half of the interviewees also supplied examples of the graphics they use to convey their metrics to senior management.

After each metric summary comes an evaluation. Each metric was scored against the Security Metrics Evaluation Tool (Security MET) by two members of the project's expert panel and one member of the research team. The outside experts are high-level security professionals who currently use metrics, and the researcher was especially well-equipped to focus on each metric's methodological (technical) aspects. Their scores are presented in a score sheet. The two outside experts reviewing each metric also supplied written comments about the metric. Those comments are condensed and provided below the score sheets. The scoring and written evaluations are meant to help readers see where they might strengthen any of these metrics if they chose to import a similar metric into their own organizations.

The summaries that follow may serve as examples for security professionals considering ways to use metrics. Combining the summaries with scoring and expert reviews provides insights not only into the metrics but also into the use of the Security MET.

For privacy, names have been left out of the summaries. The interview format (used when collecting the information) is preserved in the summaries so that readers can compare metrics against particular questions.

The metrics summarized in this section measure a variety of issues and come from a variety of industries and locations:

Metrics Collected and Evaluated
<table>

1. Office Space Usage Metric
2. Security Activity Metric
3. Environmental Risk Metric
4. Averted External Loss Metric
5. Security Audit Metric
6. Officer Performance Metric Panel
7. Security-Safety Metric
8. Security Incidents Metric

9. Personnel Security Clearance Processing Metric
10. Loss Reduction/Security Cost Metric
11. Operations Downtime Reduction Metric
12. Due Diligence Metric
13. Shortage/Shrinkage Metric
14. Phone Theft Metric
15. Security Inspection Findings Metric
16. Infringing Website Compliance Metric

Sources of Metrics	
Industries	**Locations**
Defense/Aerospace Energy/oil Finance/banking Government Insurance Manufacturing/industrial products Pharmaceutical Real estate management Retail Security services Shipping/logistics Telecom	United States Europe Australia/Asia Pacific Africa

The metric summaries attempt to provide the information needed to assess the metrics by using the Security Metrics Evaluation Tool (Appendix A). They do not capture every detail of each metric's creation and application, and they are based on self-reporting rather than external audit. Not all the metrics described here would meet the strictest definition of metrics (as opposed to simple measurements), and some may use security data for purposes other than traditional security. Nevertheless, the summaries are intended to provide examples of actual metrics in use in the field, with enough detail to determine how they measure up against the Security MET.

1. Office Space Usage Metric

1. **Respondent title**

   - CPP, PCI, PSP, Regional Security Manager

   - Security Manager–Americas

2. **Organization's geographic location, field/industry, number of employees, number of sites, annual revenue (or other measure of size)**

   The metrics apply to approximately 100 sites in the Americas. Field: communications equipment; 72,000 employees worldwide; sales: $19 billion.

3. **Description of metric (what are you measuring, and in general why?)**

   With our access control systems, we do an unusual form of attendance tracking that is very valuable to the corporation.

   In the course of measuring many security-relevant activities and incidents, we also track access to our facilities by employees and contractors. We are not using this data for normal time and attendance or payroll purposes. Rather, we count up to one entry per person per day to help the corporation understand usage patterns at these facilities. That data leads to a percentage of site use for each person (e.g., Mr. Jones uses his desk approximately 1 workday out of 10). This metric helps the corporation decide whether more, less, or different office space is needed at a given site.

   Experience shows that claimed attendance is different from measured attendance, and site managers are reluctant to give up space. Having a solid metric regarding each person's use of office space helps the corporation pay for only as much space as is needed. "Hoteling," the practice of sharing office space, is more cost-effective when genuine usage figures are known. For example, if a person says he uses his office 4-5 days a week, he may not be able to share the space, but if he actually uses it only 1-2 days per week, the space may be shareable.

   This metric, provided by security management, is extremely valuable to senior management. We track the actual savings from renegotiated contracts for space leases. The metric provides a clear economic benefit.

4. **How long has the metric been used at the organization?**

   Approximately four years.

5. **How reliable is the data you collect for the metric? Please explain.**

   The data is very reliable. It is based on actual access to the site as measured by our access control systems. Moreover, people want to be counted so they take care to swipe in correctly.

6. **How do you ensure that the conclusions you draw from your metric are valid? Please explain.**

   There is a clear correlation between the number of days a user swipes into a building and the number of days a person is present at the building. If a person rarely swipes into the building, he or she rarely uses that space.

7. **Would your metric be useful to other organizations? In other words, is it generalizable?**

   Yes and yes.

8. **What is the cost of developing and administering your metric? This includes monetary and non-monetary costs associated with metric development and administration, as well as any negative consequences associated with collecting the data or using the metric (for example, data collection takes a lot of staff time or offends employees).**

   Data collection is not difficult. We collect it from our several access control systems. The number crunching takes some time. It takes one analyst a week or more of part-time work.

   Not all of our sites are on the same access control system, so we use Crystal Reports, a business intelligence application from SAP, to consolidate data from several sources. Crystal Reports also helps us design and generate reports. Sometimes we create simple Excel spreadsheets.

9. **Can the data for your metric be collected in a timely fashion—so it is relevant for decision-making?**

   We collect and analyze the data monthly. The metric is collected and provided promptly—finished about two weeks past the turn of each month—so it can be used for decision-making.

10. **Could people fake the metric data if they wanted to? Is there any incentive for them to do so?**

    It would be hard to fake the data. Possibly an employee who rarely goes to an office could give his access card to a fellow employee and ask him to swipe it across the access sensor when the first employee is not present, but that would require collusion and ongoing execution of the con.

11. **Can your metric be used to demonstrate a return on security investment?**

    Yes—the corporate savings from more efficient allocation of office space are significant. We can show that beyond the hard-to-quantify return from our access control systems (in terms of risk reduction and crime prevention), the access control systems are also valuable for space allocation, which clearly saves money.

12. **Is the metric aligned with your organization's goals, mission, objectives, assets, or risks? How?**

    The metric is directly aligned with the organization's goal of cost savings and not wasting assets (office space).

13. Are your metric and metric results easy to explain to others—especially to senior management?

The metric is simple. If a person comes to the building only 20 percent of the time, he probably does not need his own private office space there.

14. How do you use the metric? What does it do for you? Does it guide your security decision-making?

Specifically, if our reports show that a particular employee is using his or her office space less than 40 percent of the time, the real estate division initiates a discussion with site management regarding space savings. Generally, the real estate division bases its decision on a six-month span of data (to distinguish an unusual period of absence from a genuine trend).

Interestingly, because employees and contractors want their attendance to be counted (for space allocation purposes), they tend to avoid piggybacking; they all want to swipe their cards at the reader. Thus, this metric has the effect of increasing compliance with an important security practice—badging in and out.

15. Can you share specifics—for example, specific measurements over time, specific security changes you made in response to the metric, and whether those changes had the desired effect?

The company routinely makes office allocation decisions based on this metric, clearly saving money.

Scoring and Comments from Reviewers

Based on the Security Metrics Evaluation Tool (Security MET)

Metric 1	Researcher	Expert 1	Expert 2	
Criterion	Score	Score	Score	Average
1. Reliability	5	4	3	4.00
2. Validity	5	4	1	3.33
3. Generalizability	3	3	5	3.67
Technical Total	**13**	**11**	**9**	**11.00**
4. Cost	3	3	3	3.00
5. Timeliness	5	3	5	4.33
6. Manipulation	4	3	3	3.33
Operational (Security) Total	**12**	**9**	**11**	**10.67**
7. Return on Security Investment	5	5	1	3.67
8. Organizational Relevance	5	5	1	3.67
9. Communication	5	3	5	4.33
Strategic (Corporate) Total	**15**	**13**	**7**	**11.67**
TOTAL ACROSS CRITERIA	40	33	27	33.33

Expert comments: This is an excellent metric that provides quantifiable, actionable space utilization data that directly impacts the overhead expenses in managing a business. The data also supports the return on investment associated with automated facility access control systems. The user will need to communicate the metric carefully so as not to offend line employees; also, managers might feel the metric undermines their authority.

2. Security Activity Metric

1. **Respondent title**

   - CPP, PCI, PSP, Regional Security Manager

   - Security Manager–Americas

2. **Organization's location, field/industry, number of employees, number of sites, annual revenue (or other measure of size)**

   The metrics apply to approximately 100 sites in the Americas. Field: communications equipment; 72,000 employees worldwide; sales: $19 billion.

3. **Description of metric (what are you measuring, and in general why?)**

   We use a panel of measurements to create a broad security activity metric. We measure such items as:

   - visitors: preregistered and other

   - alarm responses

   - door openings

   - material bearer passes

   - security incidents

   - other events

   - several other officer security activities

   Purpose: to adjust security resource expenditures (especially security officer staffing and security equipment/automation) up or down as needed, based on objective measurements.

4. **How long has the metric been used at the organization?**

   At least four years.

5. **How reliable is the data you collect for the metric? Please explain.**

   Much of the data is collected automatically. We have no reason to think the numbers are wrong.

6. **How do you ensure that the conclusions you draw from your metric are valid? Please explain.**

   The data seems closely related to how busy the sites and security officers are and hence how many officers are needed.

7. **Would your metric be useful to other organizations? In other words, is it generalizable?**

   The concept is generalizable—security staffing and technology needs are related to the level of activity at a site. However, we have not created an objective number or ratio that connects the level of activity to the number of officers needed at a site. Another organization could use our method but might interpret the results differently.

8. **What is the cost of developing and administering your metric? This includes monetary and non-monetary costs associated with metric development and administration, as well as any negative consequences associated with collecting the data or using the metric (for example, data collection takes a lot of staff time or offends employees).**

   Most of the data is easy to collect. Access data (regarding employees, visitors, customers, and others) is generated by our electronic access control systems. Security officer activity data is already being tracked. Some data comes to us automatically, while other data must be provided by site managers. Overall, it is not particularly time-consuming, difficult, or obnoxious to collect the data we need.

9. **Can the data for your metric be collected in a timely fashion—so it is relevant for decision-making?**

   Yes, we get the data quickly.

10. **Could people fake the metric data if they wanted to? Is there any incentive for them to do so?**

    It is possible to fake some of the data, but doing so would take work, and the incentive to fake it is not great.

11. **Can your metric be used to demonstrate a return on security investment?**

    It is common for us to determine, through the metric, that because little activity takes place at a site, we can reduce or eliminate uniformed security officers there. That is a quantifiable return on investment.

12. **Is the metric aligned with your organization's goals, mission, objectives, assets, or risks? How?**

    The metric is aligned with the organization's general goals of reducing risk (through security) and controlling costs.

13. **Are your metric and metric results easy to explain to others—especially to senior management?**

    Yes. We use our metric to support requests for security expenditures. We present the metric to senior management in security and all the way up to the chief operating officer.

14. **How do you use the metric? What does it do for you? Does it guide your security decision-making?**

    The metric enables us to deploy the right level of security measures for a site. We adjust staffing, automation, and equipment based on a genuine knowledge of what is happening at each site. That way, we avoid overdoing security (wasting money) and underdoing security (leaving sites
    at risk).

15. **Can you share specifics—for example, specific measurements over time, specific security changes you made in response to the metric, and whether those changes had the desired effect?**

    Basically, we have adjusted security expenditures up or down as needed. It seems to be working.

Scoring and Comments from Reviewers

Based on the Security Metrics Evaluation Tool (Security MET)

Metric 2	Researcher	Expert 1	Expert 2	
Criterion	**Score**	**Score**	**Score**	**Average**
1. Reliability	5	4	4	4.33
2. Validity	4	3	4	3.67
3. Generalizability	3	4	3	3.33
Technical Total	**12**	**11**	**11**	**11.33**
4. Cost	4	4	3	3.67
5. Timeliness	4	4	5	4.33
6. Manipulation	3	3	3	3.00
Operational (Security) Total	**11**	**11**	**11**	**11.00**
7. Return on Security Investment	4	2	5	3.67
8. Organizational Relevance	5	3	5	4.33
9. Communication	5	4	5	4.67
Strategic (Corporate) Total	**14**	**9**	**15**	**12.67**
TOTAL ACROSS CRITERIA	**37**	**31**	**37**	**35.00**

Expert comments: This organization has achieved an efficient and effective method of capturing relevant data and quantifying necessary security resources based on that data. The data sources based on automated systems and processes are highly reliable and verifiable, while some other data sources in the metric are more subjective. The metric is easy to explain to senior management, yet its ROI claims focus on reducing security costs and may not be able to make the case for greater security investment when necessary.

3. Environmental Risk Metric

1. **Respondent title**

   Assistant Vice President, Corporate Security

2. **Organization's location, field/industry, number of employees, number of sites, annual revenue (or other measure of size)**

   Insurance company in Midwest U.S.; revenue approximately $18 billion; hundreds of owned and leased facilities throughout the United States.

3. **Description of metric (what are you measuring, and in general why?)**

   This metric is designed to serve the risk management needs of the corporation. We [corporate security] have not named the metric, but it could be called an environmental risk metric.

   Our company owns or leases hundreds of facilities across the United States. They include offices, data centers, retail storefronts, and claim centers. On a regular basis, corporate security collects a suite of data, assigns weights to various factors, and develops a numeric score that places each facility into a low, medium, or high category of risk. For each risk category, written policy specifies a collection of security measures that should be in place at the site. Exceptions can be granted, but the systematic approach results in uniformity and in efficiency in decision-making and security systems contracting. Most important, the metrics-based approach helps senior management understand the level of risk in site selection and make informed decisions on risk management. In addition, over time, the metrics have steered the corporation toward having a smaller percentage of its locations in high-risk sites.

   The formula for our ongoing risk assessment metric is as follows:

   CAP Index Score (local risk analysis) [CAP Index is a commercial provider of crime risk forecasting. CAP stands for Crimes Against Persons and Crimes Against Property.]

   The average national crime rating score through CAP is 100. CAP is valued as follows:

   1 – CAP score of 100 or lower.

   2 – CAP score of 101 to 200.

   3 – CAP score of 201 to 300.

   4 – CAP score of 301 to 400.

   5 – CAP score of 401 to 500.

   6 – CAP score of 501 to 600.

   Locations with a score of 601 or more will not be considered as a location for an office. Industry benchmark indicates that only 7% of financial services offices are located in areas with a score of 600 or more

Type of environment:

1 – Non-critical: storage, empty space, surplus equipment. Locations that, if rendered inoperable, would have little or no negative impact on business processes.

3 – Sensitive: administrative, claims, trial office, sales office or other public contact. Locations that, if rendered inoperable, could have their work transferred to another location with little impact to the business.

5 – Mission critical: IT/data center, call center, headquarters. Locations that, if rendered inoperable, would negatively impact the business for an extended period.

Sensitivity of the asset:

1 – Low: Nothing of irreplaceable value including non-identifying records, furniture, low value equipment, perishable supplies, surplus assets. Facility may not be identified/branded as a corporate asset.

3 – Medium: Valuable equipment, associates, personally identifying records. Facility is branded as a corporate asset.

5 - High: Critical information/data, leadership associates, board members, cash/cash equivalents, and critical infrastructure. Facility is identified as an integral part of the corporation, branded and well known in the community.

Occupancy type:

1 – Unoccupied space

2 – Mixed tenant space

3 – Sole tenant

The risk levels are defined by the following total scores from the values above:

Low-risk location = 4 to 9 points

Medium-risk location = 10 to 15 points

High-risk location = 16 to 19 points

Corporate policy defines the security measures required at each level of risk.

4. How long has the metric been used at the organization?

12 years.

5. How reliable is the data you collect for the metric? Please explain.

Most of the data is objective. The CAP Index score comes from an outside source. Defining the use of the site (storage, data center, etc.) is fairly straightforward. Site sensitivity depends on contents, which are listed in the policy. Occupancy type is straightforward. The data seems reliable.

6. **How do you ensure that the conclusions you draw from your metric are valid? Please explain.**

   Every quarter I present our conclusions to the corporate risk committee. We compare our loss and incident history to our policy. We follow the numbers over time. We are then able to compare our plan, and the site ratings, to reality.

7. **Would your metric be useful to other organizations? In other words, is it generalizable?**

   I believe so, with customization.

8. **What is the cost of developing and administering your metric? This includes monetary and non-monetary costs associated with metric development and administration, as well as any negative consequences associated with collecting the data or using the metric (for example, data collection takes a lot of staff time or offends employees).**

   In terms of non-monetary costs, the metric seems clean—no negative consequences. We pay $130 for a CAP Index score, per location. The initial design of our data collection system for this metric required a significant amount of administrative time. There is also the ongoing monitoring of incidents. However, the ongoing cost is minimal.

9. **Can the data for your metric be collected in a timely fashion—so it is relevant for decision-making?**

   Yes, it is timely. Much of the process is automated. We use a Lotus Notes database to compile the data. The data comes in constantly.

10. **Could people fake the metric data if they wanted to? Is there any incentive for them to do so?**

    People could conceivably fake the data, but that would mean lying about verifiable facts—a fairly serious move. We feel the data is good.

11. **Can your metric be used to demonstrate a return on security investment?**

    Yes, in two ways. First, through the standardization that the policy calls for, we can spend right, obtaining long-term national contracts at good prices (e.g., alarm monitoring). Second, in our company's associate engagement survey, employees have responded that they feel safe in our facilities, and that they can work better when they feel safe. Thus, our metric, which increases site safety, also improves employee morale and productivity as is measured by survey.

12. Is the metric aligned with your organization's goals, mission, objectives, assets, or risks? How?

One of my goals is to help the organization decide on its security risk appetite. I try to get senior leadership to pay attention and help decide how much risk to accept.

We had guidelines before. Now we have *policy*.

We're an insurance company. We like to keep people safe and minimize loss. This metric puts our security work into a language—risk—that senior management can understand.

13. Are your metric and metric results easy to explain to others—especially to senior management?

I create a PowerPoint with graphs and tables (included below). It is easy for senior management to understand.

14. How do you use the metric? What does it do for you? Does it guide your security decision-making?

The metric helps senior management place facility site risk in perspective. Over time, it steers our site selection toward safer areas. The metric also gives us uniformity in specifying site security measures, provides economies of scale in contracting, and measurably adds to employee feelings of safety at work.

15. Can you share specifics—for example, specific measurements over time, specific security changes you made in response to the metric, and whether those changes had the desired effect?

Since we instituted the metric, security measures at headquarters have been accompanied by a roughly 50 percent decline in security incidents there.

Enterprise Physical Security Risk Dashboard

The following is an example of a graphic we would present to senior management:

YTD Critical Events

➢ XYZ location officers saved an associate's life during a heart attack. Officers across the company intervened in 12 assaults to save people from serious harm.

➢ An armed assailant led police through the downtown district only to be captured with the assistance of our officers.

➢ 13 high risk threats to the workplace and/or our associates were successfully de-escalated by the IMT.

➢ Security officers extinguished 12 fires.

	Laptop Theft	Assault	Threats
Overview	Laptops are the most stolen item across company. These thefts are primarily due to unsecured devices left in associate cars	The areas around our largest campuses have seen a slow increase in the number of assaults on the public who may be visiting these areas	Threats can come from claimants, policy holders, associates, and family members. Threats are directed against our facilities, associates, and agents
Sources	External	External	Both internal and external
Trend	Continues on pace with previous years	After a low in 2011 we have seen increases in 2012 and 2013.	After an exceptionally light year in 2012 threats have quadrupled in number. Significant assets are used to investigate and mitigate these threats

CAP Score (Crime Risk) Distribution Across All Sites

Site Count (70, 60, 50, 40, 30, 20, 10, 0)

CAPS Score Ranges: 0-100, 101-200, 201-300, 301-400, 401-500, 501-600, 601-700, 701-800, 801-900, 901-1000, 1001-1100

CAP Risk Distribution Vs. Industry

- Low
- Medium
- High

(Industry, Us)

Scoring and Comments from Reviewers

Based on the Security Metrics Evaluation Tool (Security MET)

Metric 3	Researcher	Expert 1	Expert 2	Expert 3	
Criterion	Score	Score	Score	Score	Average
1. Reliability	4	3	4	5	4.00
2. Validity	4	3	4	5	4.00
3. Generalizability	3	4	4	5	4.00
Technical Total	**11**	**10**	**12**	**15**	**12.00**
4. Cost	3	5	5	3	4.00
5. Timeliness	5	5	5	5	5.00
6. Manipulation	4	4	4	5	4.25
Operational (Security) Total	**12**	**14**	**14**	**13**	**13.25**
7. Return on Security Investment	5	2	3	5	3.75
8. Organizational Relevance	5	5	5	5	5.00
9. Communication	5	4	4	5	4.50
Strategic (Corporate) Total	**15**	**11**	**12**	**15**	**13.25**
TOTAL ACROSS CRITERIA	**38**	**35**	**38**	**43**	**38.50**

Expert comments:

This is a useful tool for determining the risk associated with various sites and determining what security controls should be in place at each location. Ongoing review of CAP scores provides continuous evaluation. It might be beneficial to add other data sources to the metric, as well. The metric is straightforward, easy to maintain, and fairly easy to understand. Tying it to organizational policy increases the likelihood of consistent implementation of security measures.

4. Averted External Loss Metric

1. **Respondent title**

   CPP, Director of Corporate Security

2. **Organization's location, field/industry, number of employees, number of sites, annual revenue (or other measure of size)**

   U.S. Midwest, distributor of products for use in business facilities (business-to-business sales), $9.3 billion annual revenue, 21,000 employees

3. **Description of metric (what are you measuring, and in general why?)**

   We measure averted losses from fraudulent orders. We quantify the losses prevented via security intervention.

   In our business, the biggest loss risk is external. We track external risks in three categories:

   - fraud through new or existing accounts (accounts that other businesses—our customers—have established for purchasing products from us)

   - fraud through e-commerce (that is, via our website)

   - fraudulent orders placed with credit cards

   We examine all three categories of risk for fraud losses. We present our impact in terms of averted losses—that is, identified high-risk orders that were examined, found to be likely fraudulent, and subsequently stopped. Orders may be stopped before shipping or even while in transit.

4. **How long has the metric been used at the organization?**

   Approximately five years.

5. **How reliable is the data you collect for the metric? Please explain.**

   We use a service called Accertify, a subsidiary of Amex. It is a rule-based risk scoring application. It assesses orders for purchase, highlighting higher-risk orders so that we can focus our prevention efforts effectively. It is straightforward and reliable, and it provides automated data.

   Chargeback data, which helps us estimate averted losses, comes directly from our bank.

6. **How do you ensure that the conclusions you draw from your metric are valid? Please explain.**

   We derive our metric—averted losses—from objective, third-party sources, via an automated process. Our security efforts to address high-risk orders result directly and measurably in averted losses.

7. **Would your metric be useful to other organizations? In other words, is it generalizable?**

   This metric especially applies to companies engaged in business-to-business transactions. However, elements of it would apply to any company that engages in Internet sales.

8. **What is the cost of developing and administering your metric? This includes monetary and non-monetary costs associated with metric development and administration, as well as any negative consequences associated with collecting the data or using the metric (for example, data collection takes a lot of staff time or offends employees).**

   Costs include the following:

   - Purchase of fraud-detection software, plus a cost per transaction

   - Time spent by fraud analysts in our financial services organization

   - Time spent by security staff

   Over time, the process becomes more automated, and staff time requirements diminish.

9. **Can the data for your metric be collected in a timely fashion—so it is relevant for decision-making?**

   We receive ongoing, real-time data from the fraud-detection software. We produce monthly totals and year-to-year comparisons.

10. **Could people fake the metric data if they wanted to? Is there any incentive for them to do so?**

    No. The data is system-generated.

11. **Can your metric be used to demonstrate a return on security investment?**

    Yes. Averted losses represent a quantitative benefit expressed in monetary terms, and that benefit is closely tied to our efforts to identify and prevent fraudulent orders.

12. **Is the metric aligned with your organization's goals, mission, objectives, assets, or risks? How?**

    Yes. This metric helps senior management properly estimate the risk associated with various ways of conducting business. For example, our ongoing metric regarding losses averted from several types of fraud (accounts, e-commerce, and credit card fraud) helps senior management develop corporate strategy, in particular by helping to quantify the risks associated with e-commerce.

13. **Are your metric and metric results easy to explain to others—especially to senior management?**

    We communicate this metric to the field (branches of our company), the C-suite, the audit committee, and the board of directors.

We report averted losses to a wide audience via our monthly security report. Quarterly, we report averted losses to the audit committee. That report has high visibility and high impact.

14. How do you use the metric? What does it do for you? Does it guide your security decision-making?

Metric data directly guides the security department's investigative efforts. The metric itself—losses averted in various categories of business—helps senior management assess risk and develop corporate strategy.

15. Can you share specifics—for example, specific measurements over time, specific security changes you made in response to the metric, and whether those changes had the desired effect?

In the following graphic, the chart at lower left shows our substantial increase in averted losses over time, leading to savings in the millions of dollars.

Burglaries and Upgraded Branches

235 branch security upgrades completed in 2008 have driven burglaries lower. Goal is steady rate with additional upgrades installed on an as-needed basis.

Impact of EAS on Shoplifting

shoplifting incidents — # of branches with EAS Systems

Averted Losses

Guest check-out filters have helped increase averted losses. New automated fraud solution implemented in 2013 will goal of 50% fraud reduction.

International Security Support

Int Security Trainings — Int Branch Inspections

International branch inspections will increase in 2013.

Scoring and Comments from Reviewers

Based on the Security Metrics Evaluation Tool (Security MET)

Metric 4	Researcher	Expert 1	Expert 2	
Criterion	Score	Score	Score	Average
1. Reliability	5	4	5	4.67
2. Validity	5	3	3	3.67
3. Generalizability	3	1	5	3.00
Technical Total	**13**	**8**	**13**	**11.33**
4. Cost	2	3	5	3.33
5. Timeliness	5	4	5	4.67
6. Manipulation	5	3	5	4.33
Operational (Security) Total	**12**	**10**	**15**	**12.33**
7. Return on Security Investment	5	4	3	4.00
8. Organizational Relevance	5	5	5	5.00
9. Communication	5	5	5	5.00
Strategic (Corporate) Total	**15**	**14**	**13**	**14.00**
TOTAL ACROSS CRITERIA	**40**	**32**	**41**	**37.67**

Expert comments: Averted loss is a solid metric that is useful for businesses in detecting and minimizing transactional fraud. While it allows the security staff to be proactive, it needs to be carefully managed to ensure a high level of correlation between the indicators and actual fraud. Stopping or questioning orders in progress can have a very negative impact on customer satisfaction and loyalty if the fraud indicators are not accurate or the system produces too many false positives.

5. Security Audit Metric

1. **Respondent title**

   - Business Process Manager, Global Security Services

   - Security System Data Analyst

2. **Organization's location, field/industry, number of employees, number of sites, annual revenue (or other measure of size)**

   Nationwide, defense/electronics/engineering, 68,000 employees, $24 billion in sales

3. **Description of metric (what are you measuring, and in general why?)**

   This is a panel of measurements—primarily measures of compliance with customer policies regarding information assets and containers. The measurements are based on our internal security audits. Examples of deficiencies counted are information containers left open when they should be locked and noncompliance with password protocols. We gather this metric to preserve our business, as excessive deficiencies discovered during official (government) audits would cause us to lose customers.

   Here is the philosophy behind our metric:

   In a nutshell, you can pay for failure (security breaches) or you can pay for prevention. The potential failure cost here is huge. We replace failure cost with process/prevention costs, which are both lower and more predictable (and hence more budgetable).

   We base our approach on the "cost of poor quality" concept as described in Juran's Quality Handbook. One can substitute "security" for "quality" throughout. Key concepts that we follow:

   - **External failure costs.** In security terms, this could be data spills, classified data or design information getting into enemies' hands, etc. The costs in this category could be immense, and you can't plan or budget for them.

   - **Internal failure costs.** In security terms, these are the costs of cumbersome self-inspections; other inefficient processes; bad Defense Security Service vulnerability assessment scores; lots of rework of mismarked documents; or fixing of incorrect settings on a classified information system. Some of the inefficiency could result in late shipments, which could be classified as an external failure cost. This category could still involve lots of cost, but it should be more predictable.

   - **Appraisal costs.** The next step is to reduce the internal failure costs by moving the inspection earlier in the process. Doing audits on a sampling basis is a good way to find the trouble spots. Putting your attention here should reduce the high internal failure costs in exchange for budgetable appraisal.

- **Prevention costs.** The focus of internal audits evolves from product compliance to process and system compliance, a much more forward-thinking approach. If you are spending money on process audits and are using the data correctly, you are actually saving money because your failure costs are minimized or eliminated. Training and error-proofing can also be considered prevention costs.

4. **How long has the metric been used at the organization?**

   Several years.

5. **How reliable is the data you collect for the metric? Please explain.**

   It is collected by independent auditors, not by the various program directors. It appears to be reliable.

6. **How do you ensure that the conclusions you draw from your metric are valid? Please explain.**

   There is a clear relationship between our conclusions (internally discovered violations of customer security requirements) and the risk of failing external audits. If we find deficiencies, we can rightly conclude that the deficiencies exist and that correcting them promptly (before external audits) will result in more favorable scores from external auditors and hence preservation of business.

7. **Would your metric be useful to other organizations? In other words, is it generalizable?**

   This metric, properly customized, would apply to almost any organization, especially one that is subject to external audit.

8. **What is the cost of developing and administering your metric? This includes monetary and non-monetary costs associated with metric development and administration, as well as any negative consequences associated with collecting the data or using the metric (for example, data collection takes a lot of staff time or offends employees).**

   The security audits are not costly—they are our regular business.

   We recently reduced the number of security audits per year, reducing the burden on employees.

9. **Can the data for your metric be collected in a timely fashion—so it is relevant for decision-making?**

   Yes. The information is collected three times a year and is compiled quickly.

10. **Could people fake the metric data if they wanted to? Is there any incentive for them to do so?**

    The security audits are conducted by independent auditors, not by the various program directors. The independent auditors should not have an incentive to fake the data.

11. Can your metric be used to demonstrate a return on security investment?

One particular use of the metric shows a very clear ROI. We were performing security audits four times per year, but analysis of our findings suggested that we could cut the audits back to three times per year. That change reduced the burden on all employees and enabled us to reallocate our security resources. Further analysis of the audit metrics over time showed that security weaknesses ("findings") did not increase. Thus, we reduced costs and administrative burdens and did not increase risk to the corporation.

Most likely, a much larger return on investment comes from our reduction of the likelihood of external and internal failures. However, here the ROI is harder to quantify. Our customers require certain security practices. If we fail to carry out those practices, the consequences are huge, ranging from loss of business to loss of U.S. defense capabilities. Government audits determine whether we are in compliance with the required practices. To optimize our scores in government audits, we perform our own audits to detect and correct problems first. Thus, our security audit metrics reduce the likelihood of certain types of highly significant losses.

12. Is the metric aligned with your organization's goals, mission, objectives, assets, or risks? How?

The metric is directly aligned to corporate survival, risk management, and cost saving. The metric enabled us to save resources.

The metric helps us keep our customers happy. High security compliance may help distinguish us from our competitors.

13. Are your metric and metric results easy to explain to others—especially to senior management?

We first determine what is significant. Different leaders like different presentations. We summarize our findings and do not bother executives with trivial information. "Risk charts" (see attached) resonate with senior management. We show the probability and severity of potential events and then present our risk mitigation strategy.

14. How do you use the metric? What does it do for you? Does it guide your security decision-making?

One: We have used the metric to reduce the number of times per year that we perform security audits.

Two: We use the metric to improve compliance with customer security requirements.

On an ongoing basis we use the metric to create a friendly rivalry between program directors, who work to minimize the number of violations.

We use changes in the metric to guide our security awareness efforts. We also present the metric data in our awareness campaigns.

15. Can you share specifics—for example, specific measurements over time, specific security changes you made in response to the metric, and whether those changes had the desired effect?

We were able to reduce the frequency of audits.

For presentations to senior executives, security managers place various risks into the correct boxes to show likelihood and severity of occurrence. Colors represent seriousness of the risk in terms of DSS (Defense Security Service) actions.

Risk Chart

Will result in a **Serious DSS finding** if proper action not taken

Will result in a **Repeat Systemic DSS finding** if proper action not taken

Will result in an **Administrative DSS finding** if proper action not taken

Scoring and Comments from Reviewers

Based on the Security Metrics Evaluation Tool (Security MET)

Metric 5	Researcher	Expert 1	Expert 2	
Criterion	Score	Score	Score	Average
1. Reliability	4	4	5	4.33
2. Validity	5	3	4	4.00
3. Generalizability	4	5	4	4.33
Technical Total	**13**	**12**	**13**	**12.67**
4. Cost	4	2	3	3.00
5. Timeliness	4	4	4	4.00
6. Manipulation	5	4	4	4.33
Operational (Security) Total	**13**	**10**	**11**	**11.33**
7. Return on Security Investment	4	4	4	4.00
8. Organizational Relevance	5	4	5	4.67
9. Communication	4	4	4	4.00
Strategic (Corporate) Total	**13**	**12**	**13**	**12.67**
TOTAL ACROSS CRITERIA	**39**	**34**	**37**	**36.67**

Expert comments: Overall, the security audit metric provides a high level of reliability and validity when determining compliance with customer policies. The correlation between internal security violations, found prior to an external audit, and costs savings is very precise. In providing this information to the C-suite, by using established theories, such as *Juran's Quality Handbook*, the metric has more generalized applicability and assists with the presentation process.

The metric is useful for proving that the organization can obtain the same results with fewer audits. Depending on how one views the costs, data collection may actually cost more than the summary suggests.

6. Officer Performance Metric Panel

1. **Respondent title**

   CPP, Vice President, Growth & Contract Management

2. **Organization's location, field/industry, number of employees, number of sites, annual revenue (or other measure of size)**

   Southern U.S., contract security officer service, 1,600 employees, $37 million revenue

3. **Description of metric (what are you measuring, and in general why?)**

   We measure several characteristics of the contract security officers whom we supply to customers. The complete composition and weighting of the metrics panel is proprietary, but in general we measure such items as:

   - employee turnover

   - employee safety incidents (OSHA) on customer property

   - safety/security incidents such as theft and/or vandalism on client property

   - time from notice of need to response 'on site'

   - number of safety 'assists' provided such as escorts, charging a dead battery, refueling, unlocks, etc. for client employees and/or visitors on client property

   - number of trainings held/conducted for each officer on site within a period

   - post audits conducted and findings such as 'refresher training needed,' 'uniform replacement needed,' 'post instructions need updating,' etc.

   - management site visits conducted per period

   - accuracy of invoicing

   Turnover by wage as well as BLS statistics are taken into account when we establish wage for a contract. Lower turnover represents improved tenure of employees for our customers, who are then willing to pay better wages. Other elements of our metrics panel prove the quality and quantity of service provided (more than just the number of hours worked).

4. **How long has the metric been used at the organization?**

   At the original client site, more than 10 years.

5. **How reliable is the data you collect for the metric? Please explain.**

   Data is collected from actual occurrences only, meaning there must be a form of documentation that the event actually did occur: incident report, employee assist log, post audit report, training records, etc. Therefore, the reliability of the data collected is unquestionable.

6. **How do you ensure that the conclusions you draw from your metrics are valid? Please explain.**

With the turnover data, the market validates our conclusion. New customers demonstrate a willingness to pay recommended wages because we have data/documentation to prove our point. Customers look for validation, not just recommendations so we can make more money.

When metrics are used as key performance indicators (KPIs) on a given customer site, meeting those metrics is a way of measuring whether we are meeting the customer's expectations. When we continually perform to those established metrics month after month, dollars invoiced are validated and earned based on the achievement of the KPIs.

7. **Would your metric be useful to other organizations? In other words, is it generalizable?**

Yes, we have repeated the process with several customers. But the customer has to be willing to invest time on a regular basis to review the KPIs and metrics we have collected. When the customer invests the time, it becomes a win-win situation. KPIs would need to be adjusted to the individual site based on the duties to be performed as agreed to by both customer and provider.

8. **What is the cost of developing and administering your metric? This includes monetary and non-monetary costs associated with metric development and administration, as well as any negative consequences associated with collecting the data or using the metric (for example, data collection take a lot of staff time or offends employees).**

Data collection is just a matter of tracking what we do. It's a process of accountability for those performing the job. One admin person enters the data into a centralized log for reporting purposes but the results far outweigh the cost of that person's time plus that person has other duties such as scheduling. The reports and accountability fall under the supervisors for each shift. Cost of developing and administering the metrics are inconsequential. We do NOT have any negative effects of collecting or using the metrics. It does hold everyone accountable for their job function and if they are not meeting expectations, it is a measure of knowing 'where' they fell short. So it turns out to be a positive reinforcement of where improvement should be made.

9. **Can the data for your metric be collected in a timely fashion—so it is relevant for decision-making?**

Metrics are collected daily and are readily available for any time period; week, month, quarter, etc. It's an ongoing process and is best compared to a similar period in a previous year or quarter. As for decision-making, we provide a number of "volume" metrics to help establish employee workload: number of trucks through a gate by shift, entries as compared to other shifts, delays in getting trucks cleared, etc.

10. Could people fake the metric data if they wanted to? Is there any incentive for them to do so?

There is almost always a way to fake a metric, but there is little reason to do so. Employees are not individually bonused or penalized, but rather directed on areas of improvement.

11. Can your metric be used to demonstrate a return on security investment?

With this metric we can show customers that they will receive a better service that justifies a higher price.

12. Is the metric aligned with your organization's goals, mission, objectives, assets, or risks? How?

The metric is clearly aligned with the overall goal of profitability, as it enables us to prove to customers that our services are worth more. The metric also strengthens our ability to provide high-quality service by giving us current information on officer performance.

13. Are your metric and metric results easy to explain to others—especially to senior management?

We create graphs/charts/slides/summaries etc. to inform customers about the performance quality of our officers when we renegotiate contracts.

14. How do you use the metric? What does it do for you? Does it guide your security decision-making?

Absolutely drives our decision-making as regards officers' wage increase, contract renegotiations, company-wide award fees (from the customer), etc. It provides us a way to know we are meeting our customer's expectations (customer satisfaction) and justify the dollars we invoice.

Primarily it helps us resolve conflicts without pointing fingers at individuals. We are able to define through metrics when a process or procedure has not achieved the desired result and make the necessary corrections rather than just point a finger at an individual and say "shame on you," which does not correct the problem. Metrics make it about the process or procedure rather than personality.

15. Can you share specifics—for example, specific measurements over time, specific security changes you made in response to the metric, and whether those changes had the desired effect?

We have certainly increased and/or decreased security manpower coverage based on tracked metrics, such as volume of work completed in specific functions, incidents dispatched, truck entries, badges issued, safety orientation trainings conducted, etc. We often defend the number of personnel it takes to meet safety/security requirements by providing data collected and tracked such as the number of incidents on property during various periods. No personnel on duty versus personnel on duty, armed versus unarmed, response times, etc.

Scoring and Comments from Reviewers

Based on the Security Metrics Evaluation Tool (Security MET)

Metric 6	Researcher	Expert 1	Expert 2	
Criterion	**Score**	**Score**	**Score**	**Average**
1. Reliability	5	3	5	4.33
2. Validity	5	3	4	4.00
3. Generalizability	4	3	5	4.00
Technical Total	**14**	**9**	**14**	**12.33**
4. Cost	3	2	4	3.00
5. Timeliness	5	2	4	3.67
6. Manipulation	4	3	3	3.33
Operational (Security) Total	**12**	**7**	**11**	**10.00**
7. Return on Security Investment	4	3	5	4.00
8. Organizational Relevance	5	3	4	4.00
9. Communication	5	3	5	4.33
Strategic (Corporate) Total	**14**	**9**	**14**	**12.33**
TOTAL ACROSS CRITERIA	**40**	**25**	**39**	**34.67**

Expert comments: Officer turnover is one of the vital measurement areas for security officer metrics. A strong metric is to set the officer turnover at or below the national average—e.g., security officer turnover will not exceed 16 percent per quarter. Such a metric is sound and has a direct impact on a company's bottom line (as new officers require spin-up time, training, familiarization, etc.). The data could be manipulated if the metric does distinguish between reasons for departure. Still, total turnover is the most important measurement.

7. Security-Safety Metric

1. **Respondent title**

   PSP, Security Operations Manager

2. **Organization's location, field/industry, number of employees, number of sites, annual revenue (or other measure of size)**

   U.S. Midwest; multiple locations; aerospace/defense; 14,000 employees; $4.4 billion revenue

3. **Description of metric (what are you measuring, and in general why?)**

   We monitor numerous categories of work performed by the central station operators and security officers based in our security operations center (SOC). One category especially supports corporate risk management—security's contribution to workplace safety.

   Since the creation of our new SOC, the security department has identified serious workplace safety issues in the course of its multi-site monitoring and incident tracking. Using automated systems to collect incident and other data, we are able to report on incidents in which detection and intervention by the security department led to the mitigation of significant workplace safety risks. It is a constant battle to put a price on protection, but these safety issues are more immediate and less theoretical than possible security incidents prevented, and hence their value may be easier for senior management to envision.

   On many occasions, often with our video capabilities, we have discovered, intervened in, or tracked safety issues such as the following:

   - We detected significant water leaks in buildings and notified facilities staff.

   - We partnered with the safety department to investigate reckless forklift operators.

   - We detected and investigated on-site drug use.

   - Incident tracking helped us detect a trend in workplace injuries—namely, people falling repeatedly on a particular floor area sealed with a slick paint.

   We also measure the central functions of taking and making phone calls, coding phone calls, making badges, processing visitors and contractors, responding to alarms, completing incident reports, managing access control systems, and many more functions. We use those measures to demonstrate, quantitatively, that security staff members are performing substantial amounts of necessary work.

4. **How long has the metric been used at the organization?**

   Three years—since 2010.

5. **How reliable is the data you collect for the metric? Please explain.**

   Very reliable, as it is verifiable through video recordings, incident reports, and records of other departments. The key thing is to use automated data so that it is auditable.

6. **How do you ensure that the conclusions you draw from your metric are valid? Please explain.**

   All the numbers we use are pulled from various software sources. If we are audited, we can prove their existence and do not have to worry about padding our numbers or making things up.

7. **Would your metric be useful to other organizations? In other words, is it generalizable?**

   A little bit. I have shared it with local ASIS members.

8. **What is the cost of developing and administering your metric? This includes monetary and non-monetary costs associated with metric development and administration, as well as any negative consequences associated with collecting the data or using the metric (for example, data collection takes a lot of staff time or offends employees).**

   Time. Also, we use D3 incident reporting software.

9. **Can the data for your metric be collected in a timely fashion—so it is relevant for decision making?**

   Yes. We collect the data monthly.

10. **Could people fake the metric data if they wanted to? Is there any incentive for them to do so?**

    It is possible that someone could fake certain measurements in an effort to gain more funding for staff or equipment. However, the safety interventions that we measure would not be easy to fake.

11. **Can your metric be used to demonstrate a return on security investment?**

    Yes. Our contributions to workplace safety represent fairly tangible losses avoided: damage, injury, crime, productivity loss, etc.

12. **Is the metric aligned with your organization's goals, mission, objectives, assets, or risks? How?**

    Our central station is geared toward supporting all corporate sites, and the numbers show that the staff is working.

13. **Are your metric and metric results easy to explain to others—especially to senior management?**

    I explain the statistics, one by one, to the chief security officer. I show a slide for each category of activity or incident. Then he passes the information up the chain.

14. How do you use the metric? What does it do for you? Does it guide your security decision-making?

We use our metrics mainly to show upper management that they are getting their money's worth.

15. Can you share specifics—for example, specific measurements over time, specific security changes you made in response to the metric, and whether those changes had the desired effect?

I believe you need at least three to five years of collected stats to truly analyze the data and watch for patterns that may or may not need to be addressed or monitored for future resolution. We are almost there. Our numbers have been going up, up, up, and I'll be asking for additional staff in the future.

We use tables like the following to demonstrate our level of security activity:

| SOC Review by Month | | | | | | | | | | | | | | 2010 |
Alarms	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	TOTALS	AVG.
LENEL Alarms	45474	7117	15105	10280	7633	9428	10425	13254	21629	11609	11759	14585	178298	14858
SBN Alarms	59	3	71	122	243	83	79	167	2684	2419	6	9	5945	495
Communications														
Incoming Phone Calls	3812	3420	3907	3633	4526	4075	4082	4037	4078	4270	3791	3561	47192	3933
Access	0.4%	2.0%	3.6%	2.4%	1.5%	1.6%	0.9%	1.2%	1.8%	1.7%	2.1%	1.7%	1.7%	62
Emergency	0.1%	0.1%	0.0%	0.1%	0.2%	0.1%	0.1%	0.1%	0.2%	0.1%	0.1%	0.1%	0.1%	3
Status Report	67.0%	72.4%	68.5%	59.9%	46.7%	50.0%	52.6%	51.1%	49.8%	52.4%	57.6%	63.6%	57.0%	2028
Incident Report	0.4%	0.3%	0.4%	0.7%	0.6%	0.6%	0.5%	0.5%	0.3%	0.5%	0.4%	0.5%	0.5%	17
Condition Report	7.5%	14.0%	15.7%	25.0%	40.6%	36.6%	35.9%	34.6%	36.2%	33.0%	29.1%	22.4%	28.3%	1007
Information Request	14.4%	5.5%	7.3%	7.6%	7.7%	7.5%	6.8%	8.4%	7.9%	8.3%	7.5%	7.5%	8.0%	284
Assistance Request	1.1%	1.1%	1.5%	1.5%	1.1%	1.6%	1.5%	2.0%	2.0%	2.2%	1.5%	2.1%	1.6%	57
Other/ Misc.	9.1%	4.6%	2.9%	2.8%	1.7%	2.0%	1.8%	2.1%	1.8%	1.8%	1.8%	2.1%	2.8%	98
Outgoing Phone Calls	849	653	914	857	939	875	799	696	846	927	712	687	9754	813
Number of Abandoned Calls	97	49	162	135	171	147	147	217	152	107	50	63	1497	125
Number of Calls Transferred OUT	48	34	53	37	36	36	31	36	48	45	13	33	450	38
Number of Calls placed on HOLD	55	46	66	52	57	49	50	58	57	57	23	43	613	51
OTHER DUTIES														
LNL Cards Programmed	2140	441	159	461	327	819	1452	890	378	177	159	706	8109	676
LNL Reports Generated	231	26	31	256	696	467	709	788	590	615	738	681	5828	486
LNL Database Programming	111	27	790	346	598	82	75	558	589	104	236	432	3948	329
SBN Reports Generated	31	3	9	7	29	24	22	17	9	30	49	30	260	22
SBN Database Programming	6	1	2	2	2	0	2	2	8	5	10	5	45	4
BADGES Printed	724	23	46	77	66	342	428	123	95	62	83	77	2146	179
D3 INCIDENT Reports	6	10	15	30	35	18	26	22	21	20	17	14	234	20
D3 Work Orders Created	4	5	5	1	1	3	1	1	0	2	0	1	24	2
D3 Websense ACCESS Request	60	34	42	26	42	56	33	29	33	31	36	22	444	37
ALERTFIND Messages	0	0	0	0	0	0	0	0	0	0	0	1	1	0
EMAIL REQUESTS Completed	81	60	81	33	89	143	66	79	73	127	87	86	1005	84
These Colors Highlights Indicate the Largest Volume Months of the year 2010														

Scoring and Comments from Reviewers

Based on the Security Metrics Evaluation Tool (Security MET)

Metric 7	Researcher	Expert 1	Expert 2	
Criterion	Score	Score	Score	Average
1. Reliability	5	5	5	5.00
2. Validity	5	5	5	5.00
3. Generalizability	2	4	2	2.67
Technical Total	**12**	**14**	**12**	**12.67**
4. Cost	2	3	2	2.33
5. Timeliness	5	5	3	4.33
6. Manipulation	4	4	4	4.00
Operational (Security) Total	**11**	**12**	**9**	**10.67**
7. Return on Security Investment	5	3	3	3.67
8. Organizational Relevance	4	5	4	4.33
9. Communication	4	5	5	4.67
Strategic (Corporate) Total	**13**	**13**	**12**	**12.67**
TOTAL ACROSS CRITERIA	**36**	**39**	**33**	**36.00**

Expert comments: Safety and security often cross "swim lanes," and in the current defense market a physical security cost must be evaluated closely. Sometimes complying with a contract can helpfully spill over into protecting corporate assets. Still, return on security investment is always hard to prove. Long periods without incidents may lead senior management to wonder about the necessity for countermeasures. The return on security investment comes from catching safety issues on video and thereby preventing workplace injury lawsuits.

8. Security Incidents Metric

1. **Respondent title**

   Physical Security Program Manager

2. **Organization's location, field/industry, number of employees, number of sites, annual revenue (or other measure of size)**

   Mainly Australia, also Asia-Pacific and elsewhere in the world; more than 15,000 owned and leased physical sites in Australia; telecommunications provider; more than 38,000 employees and up to 20,000 contractors; annual revenue $25 billion ($Aus).

3. **Description of metric (what are you measuring, and in general why?)**

   We count and analyze the number and type of security incidents. Using incident management software from PPM 2000 and our own customized Web form, we have been gathering incident data to monitor losses, study the effect of security interventions, and initiate investigations.

4. **How long has the metric been used at the organization?**

   More than 25 years.

5. **How reliable is the data you collect for the metric? Please explain.**

   Data reliability varies. Some types of incidents are reported reliably, while others are not. It would be useful to link our incident reports directly with other internal systems, but cost pressures mean this is rarely done.

   Completion of a security incident report (SIR) is compulsory for some loss events. For example, a lost or stolen laptop will not be replaced unless an SIR has been completed. Thus, reporting of such losses is reliable.

   However, other types of incidents—such as damage or loss of infrastructure assets, especially cable cuts, vandalism, or theft of minor equipment—are not reliably reported. For example, for a service technician responding to a "loss of dial tone" fault, it is easier simply to repair the fault and not identify it as a crime, even if it was the result of a deliberate cable cut. Declining to report it means the technician avoids the security incident report, the police report (which must be lodged at a police station), and the "recoverable damages" report, and he can quickly move on to the next job. By skipping the reporting, technicians who are company employee can more easily meet their daily work quota. Technicians who are contractors can complete more billable jobs.

6. **How do you ensure that the conclusions you draw from your metric are valid? Please explain.**

   In a few cases, we have been able to see a clear relation between a security intervention based on metrics analysis and a decline in losses. Two examples are given below at question 16.

7. **Would your metric be useful to other organizations? In other words, is it generalizable?**

Several of our metrics would be useful to other telecommunications companies. Data relating to cable and copper theft may be applicable to power utility companies.

8. **What is the cost of developing and administering your metric? This includes monetary and non-monetary costs associated with metric development and administration, as well as any negative consequences associated with collecting the data or using the metric (for example, data collection takes a lot of staff time or offends employees).**

The only visible cost associated with the metric is the fee for a multi-user corporate software license. The costs of hosting, storage, and communication are buried in a general internal IT services support fee.

9. **Can the data for your metric be collected in a timely fashion—so it is relevant for decision-making?**

The data is collected in real time via an online form. We have "gatekeepers" who process the data as soon as it hits (during business hours) and who can follow up to confirm or seek further information, and allocate it for follow-up within minutes. To supplement our online forms, we also operate a help line, which is answered 24/7.

10. **Could people fake the metric data if they wanted to? Is there any incentive for them to do so?**

There are no rewards for reporting security incidents, so there is no incentive to exaggerate the number of issues. Reporting requires more work than not reporting, so we are more likely to see underreporting.

11. **Can your metric be used to demonstrate a return on security investment?**

In some cases we can demonstrate clear savings due to our metrics-guided security interventions. (See details at question 15.) However, overall our losses are moderate. Senior management does not consider security risk to be a major component of overall risk to the corporation, so ROI is not of great interest to them.

12. **Is the metric aligned with your organization's goals, mission, objectives, assets, or risks? How?**

The corporation's chief risk office reviewed the company's entire risk environment and determined that security risk represents 2-3 percent of the total value of risk impacts across the company. Funding for risk mitigation will be based on those findings. Our security incident metric and related security interventions are aligned with the general mission of mitigating risk. However, since security risk is small, security resources will also be small.

We were aware of the overall range of risk mitigation activities competing for operational and capital expense dollars – but had little idea of just how far down the list of priorities we were. The reality is that Australia is a comparatively benign security environment and other risk treatments will be given higher priority.

13. Are your metric and metric results easy to explain to others—especially to senior management?

Yes. We make good use of the analytics in PPM 2000's Perspective and review data further in Excel and other programs to produce visual presentations and demonstrate changes.

In my experience in Australia, the larger corporations are generally fairly good at using security metrics and the penetration of high-end access control systems is high. However, security expenditure – especially capital – is one of the first targeted when times are tough. I think the ability of security people to develop and support business cases is generally poor, especially when competing for the same funds as those looking at growing business.

As a general rule, there is a high level of sharing of security-related information amongst Australian major corporations. There is an informal network of the security managers of the "Top 100" companies, where the key focus is the business case for security.

14. How do you use the metric? What does it do for you? Does it guide your security decision-making?

Our corporate security group is not accountable for funding any security programs for the rest of the business – only its own costs. So we expend considerable effort in dealing with other parts of the business, looking at their security risks and helping them find solutions to their risk exposures. We make extensive use of our data in targeting key areas of the business in order to provide support.

15. Can you share specifics—for example, specific measurements over time, specific security changes you made in response to the metric, and whether those changes had the desired effect?

Incident tracking showed a trend of theft from field depots. In response, we installed CCTV cameras, fence alarm systems, and security lighting in locations at risk. We experienced an immediate reduction in theft.

Incident tracking metrics showed a steep rise in the cutting of communication cables linked to EFTPOS (electronic funds transfer at point of sale) transactions. After studying the metrics, we negotiated a change in bank policy so that cash-out on EFTPOS transactions would not be honored if the transaction was off-line. The graph below shows that cutting of communication cables declined precipitously after that security intervention.

Damaged Cables

Graph shows stark decline in a particular category of loss shortly after security measure was implemented.

Scoring and Comments from Reviewers

Based on the Security Metrics Evaluation Tool (Security MET)

Metric 8	Researcher	Expert 1	Expert 2	
Criterion	Score	Score	Score	Average
1. Reliability	2	4	3	3.00
2. Validity	2	4	4	3.33
3. Generalizability	3	3	3	3.00
Technical Total	**7**	**11**	**10**	**9.33**
4. Cost	2	4	4	3.33
5. Timeliness	5	4	5	4.67
6. Manipulation	3	3	3	3.00
Operational (Security) Total	**10**	**11**	**12**	**11.00**
7. Return on Security Investment	2	5	5	4.00
8. Organizational Relevance	3	5	4	4.00
9. Communication	5	5	5	5.00
Strategic (Corporate) Total	**10**	**15**	**14**	**13.00**
TOTAL ACROSS CRITERIA	**27**	**37**	**36**	**33.33**

Expert comments: This is an excellent example of a well-thought-out metric that has proven effective and reliable over time. Cost was quantifiable, and ROI was clear. On the other hand, investigative factors (e.g., inability to determine if theft was internal or external) could reduce the metric's effectiveness. Regarding costs, it can be expensive to buy software and train staff to use it, yet manual tracking could be slow and difficult. The metric shows promise for reducing pilferage, thereby enhancing the security ROI. Different companies would need to tailor this metric to their specific needs. Regular tracking, training, and reporting can be an effective means to reduce loss.

9. Personnel Security Clearance Processing Metric

1. **Respondent title**

   Senior Associate

2. **Organization's location, field/industry, number of employees, number of sites, annual revenue (or other measure of size)**

   Headquartered on east coast, U.S.; worldwide organization; defense contractor; 24,000 employees; 93 physical locations but deployed to over 200+ sites; $5.2B revenue

3. **Description of metric (what are you measuring, and in general why?)**

   Because we are a defense contractor, personnel security clearance processing is a vital step in our hiring process. We hire about 2,500 new personnel per year, but because of the length and unpredictability of the entire clearance process (both our steps and steps taken by the government), we had not generally been able to give candidates firm starting dates. Because we gave them only contingent start dates, we were losing good candidates to firms that offered firm starting dates. Moreover, each day of waiting for clearance processing was a day that the candidate could not be employed on, and billed to, a project.

   By examining the clearance process, step by step, from an enterprise point of view, we were able to

   - cut the cycle time by 50 percent (through prescreening and process improvement), getting people to work faster

   - develop a tool that tells hiring managers what start date they should offer to a candidate, strengthening our recruiting position

   - save significant sums in payroll paid before employees are billable

   - Our metric is divided into four parts. We measure the following:

   - End-to-end performance (from posting a position requirement to having a billable employee). We measure:

     - cycle time reduction

     - increase in productivity/revenue generation

     - innovations in breaking logjam (unnecessary delays in the process)

     - internal service level agreements (getting commitments to perform certain services in a certain amount of time; e.g., a visit certification will be sent in four hours or less, compared to no requirement in the past)

   - Cost/cost by market. We measure:

     - cost by security service offering

     - cost by security service offering as it relates to a market or contract

- ROI, investment vs. performance, and increased productivity/revenue generation

- job family and billing percentage (e.g., two cleared engineers billing 40 percent could be changed to one engineer billing 80 percent)

• Risk reduction. We measure:

- potential clearance delays

- reduction of contingent hires and the switch to direct hires with start dates (avoiding loss of candidates to other firms); cycle time metrics, both internal and external, are given to program managers or hiring managers so they can establish an appropriate start date

- reduction of error rates

- reduction of packages rejected because they need additional information

• Savings. We measure:

- reduction in the cost of bad hires (number of candidates identified for interview who were identified as a risk for a clearance delay X average interview process cost)

- reduction in processing staff/footprint (total budget saving, plus the ability to scale)

- reduction in overhead/sitting on the bench before clearance approval

4. How long has the metric been used at the organization?

A manual system had been used for several years but captured only half of the data above. We successfully presented the business case for capturing the personnel security clearance processing workflow and associated metrics with an automated system and dashboard for real-time metrics and performance data. We received significant funding.

5. How reliable is the data you collect for the metric? Please explain.

Extremely. The data is provided in real time, it is system-generated, and it has complete audit trails.

6. How do you ensure that the conclusions you draw from your metric are valid? Please explain.

Each subset of metrics is measured against a set of dependencies and compared with data points from various functional areas (contracts, finance, etc.). The metrics are based on direct measurement of a process. Industry benchmarks also suggest that the metrics lead to valid conclusions.

7. Would your metric be useful to other organizations? In other words, is it generalizable?

Yes, mainly to the 13,000+ defense contractor organizations.

8. **What is the cost of developing and administering your metric? This includes monetary and non-monetary costs associated with metric development and administration, as well as any negative consequences associated with collecting the data or using the metric (for example, data collection takes a lot of staff time or offends employees).**

   $3 million.

9. **Can the data for your metric be collected in a timely fashion—so it is relevant for decision-making?**

   Yes, real-time. It is used in decision-making for all new hires.

10. **Could people fake the metric data if they wanted to? Is there any incentive for them to do so?**

    No, everything has a date and time stamp or audit trail.

11. **Can your metric be used to demonstrate a return on security investment?**

    Yes.

    - 40 percent reduction in personnel security clearance processing staff/footprint

    - 50 percent reduction in personnel security clearance cycle time, equating to more than $30 million in increased productivity and revenue

    - Savings to the enterprise by hiring best-in-class candidates (reducing clearance delays) and avoiding the loss of candidates to other organizations

12. **Is the metric aligned with your organization's goals, mission, objectives, assets, or risks? How?**

    Yes.

    - 80 percent of revenue comes from cleared staff, so getting them to work faster increases revenue

    - People are our #1 asset, so a metric that leads to better hiring benefits the enterprise

    - Personnel security is considered one of the top 10 risks to the enterprise; moreover, in the event of a business disruption, the personnel security shared service center is listed among the top ten applications to get back on line

    Thus, improving the personnel security process is clearly aligned with the organization's objectives, as it addresses one of the company's top risks.

13. **Are your metric and metric results easy to explain to others—especially to senior management?**

    Yes. Nearly everything equates to cost/revenue and risk reduction while remaining compliant.

14. **How do you use the metric? What does it do for you? Does it guide your security decision-making?**

   We use it for the purposes described above and also to demonstrate the results of our work to executive staff and to gain support for continued funding for security innovations and enhancements.

15. **Can you share specifics—for example, specific measurements over time, specific security changes you made in response to the metric, and whether those changes had the desired effect?**

   Already covered above.

Scoring and Comments from Reviewers

Based on the Security Metrics Evaluation Tool (Security MET)

Metric 9	Researcher	Expert 1	Expert 2	
Criterion	Score	Score	Score	Average
1. Reliability	5	5	5	5.00
2. Validity	5	5	5	5.00
3. Generalizability	4	5	4	4.33
Technical Total	**14**	**15**	**14**	**14.33**
4. Cost	1	3	2	2.00
5. Timeliness	5	5	5	5.00
6. Manipulation	5	5	5	5.00
Operational (Security) Total	**11**	**13**	**12**	**12.00**
7. Return on Security Investment	5	5	5	5.00
8. Organizational Relevance	5	5	5	5.00
9. Communication	5	5	5	5.00
Strategic (Corporate) Total	**15**	**15**	**15**	**15.00**
TOTAL ACROSS CRITERIA	**40**	**43**	**41**	**41.33**

Expert comments: Staff understood how gaps in their program were creating unnecessary expenses. They examined their processes and developed a four-part metric that scores well on the Security MET. The cost of creating an automated, dashboard-driven data collection tool was high, but the benefit was shown to be higher. This metric is easy to understand and shows the benefits of security initiatives. It could also be useful at some point to measure personnel quality.

10. Loss Reduction/Security Cost Metric

1. **Respondent title**

   Chief Strategic Intelligence & Security Officer

2. **Organization's location, field/industry, number of employees, number of sites, annual revenue (or other measure of size**

   Based in France; shipping/logistics/supply chain; 19,500 employees; approximately 3 million square meters of sites in 12 countries; revenue €900 million

3. **Description of metric (what are you measuring, and in general why**?):

   We create a monthly dashboard of key security metrics for the company's executive committee:

   - stock discrepancy

   - security costs as a percentage of net sales

   - saving on security costs compared to budget (budgeted amounts not spent)

   These metrics are directly linked to cost savings for the company.

4. **How long has the metric been used at the organization**?

   Three years.

5. **How reliable is the data you collect for the metric? Please explain.**

   The data comes from our internal reporting databases. There can be weaknesses in the data if people do not input data into the right classifications, but overall the data seems reliable.

6. **How do you ensure that the conclusions you draw from your metric are valid? Please explain.**

   We cannot be sure our conclusions are 100 percent valid. However, our understanding seems to be close to the real situation, and with this system we are successfully decreasing losses, so it seems to work.

7. **Would your metric be useful to other organizations? In other words, is it generalizable?**

   Yes.

8. **What is the cost of developing and administering your metric? This includes monetary and non-monetary costs associated with metric development and administration, as well as any negative consequences associated with collecting the data or using the metric (for example, data collection takes a lot of staff time or offends employees).**

   Cost is only internal "time cost" and metric development by IT team and database team inside the company. At the beginning of data collection, we had some problems because employees were not in line with database processes and data collection was taking a lot of staff time. After three months of the process, we simplified the system and provided more training to staff.

9. **Can the data for your metric be collected in a timely fashion—so it is relevant for decision-making?**

   Yes.

10. **Could people fake the metric data if they wanted to? Is there any incentive for them to do so?**

    Yes, in theory, but with our system of management it is difficult. In the past, we discovered an attempt at fraud in data reporting and changed personnel.

11. **Can your metric be used to demonstrate a return on security investment?**

    Yes. Our dashboard clearly links security performance to a monetary return on investment. We also show senior management specifically how the security program brings financial benefit to the enterprise. For example:

    • Proof of loss to support enterprise insurance claims (supplied through investigative effort)

    • Actual recovery or recapture of physical assets (through investigative or patrol activity or both)

    • Establishment of claims or legal causes of action against parties other than the enterprise's own insurance carriers (investigative effort)

    • Other actions, such as recovering revenue from bad checks issued to the business

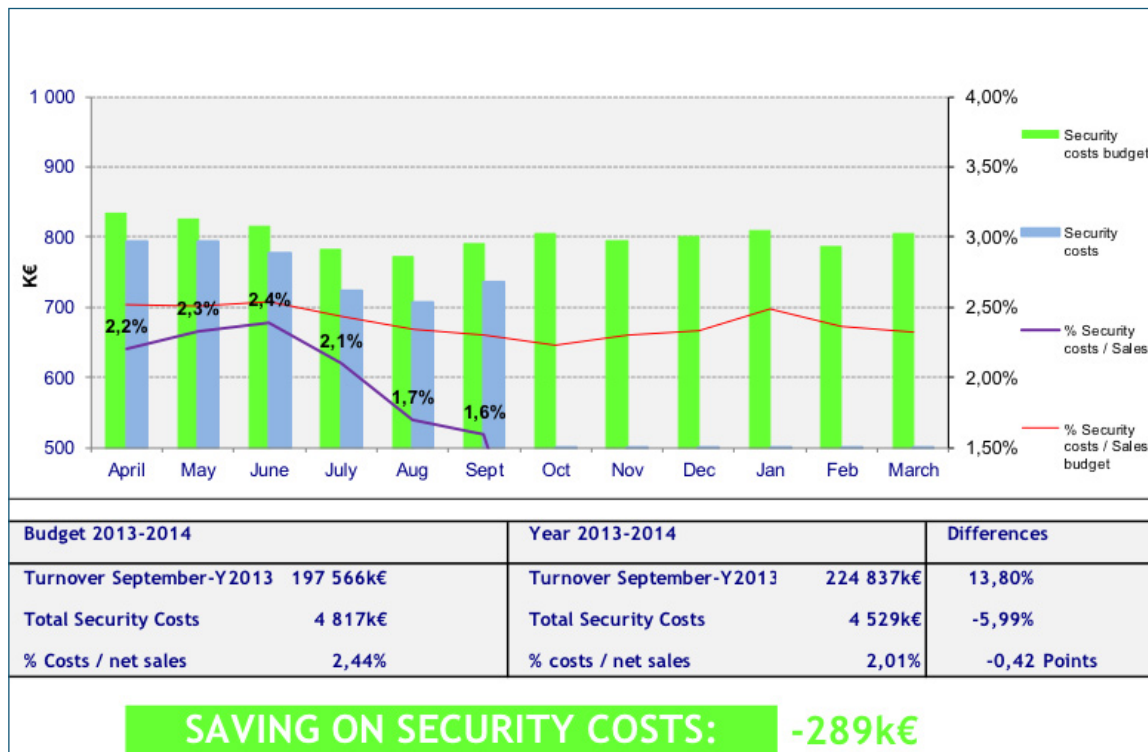12. **Is the metric aligned with your organization's goals, mission, objectives, assets, or risks? How?**

    Senior management's basic question to us in security is this: Considering the entire program and all expenses, does the assets protection function accomplish anything that can be quantified and that justifies the allocation of the funds expended? Our metric directly answers this question.

13. Are your metric and metric results easy to explain to others—especially to senior management?

Our stock discrepancy figure is stated clearly: the target value (X percent of stock lost or damaged) minus actual, measured loss/damage, which equals a quantifiable, monetary savings. For example, if the target is 0.5 percent loss or less (€1 million), and we keep losses to €600,000), then the security department has saved the company €400,000 compared to expected or budgeted losses.

Our metric on security costs as a percentage of net sales and our metric on actual versus budgeted security costs are given in a chart like this:

Budget 2013-2014		Year 2013-2014		Differences
Turnover September-Y2013	197 566k€	Turnover September-Y2013	224 837k€	13,80%
Total Security Costs	4 817k€	Total Security Costs	4 529k€	-5,99%
% Costs / net sales	2,44%	% costs / net sales	2,01%	-0,42 Points

SAVING ON SECURITY COSTS: -289k€

Note the purple line showing that security costs have been declining as a percentage of sales (actual, not budgeted). Also note the clear emphasis on under-budget security costs. Turnover in this context means sales.

Also, we use the chart below to explain to senior management why we focus on certain threats more than others:

1	Assaults against a FM employee (by an external attacker), in a warehouse or outside (FM's drivers, expatriates or business travelers)		security of people
2	Kidnap & Ransom		
3	Loss of clients' products in high quantity: in trucks or warehouses		security of material assets
4	Trucks misappropriation for criminal or terrorist attacks		
5	Arson in warehouse		
6	"Chemical" terrorist actions on storaged clients' products		
7	Financial frauds (from employees or from outside): extortion, conflict of interest, procurement fraud, etc.		security of immaterial assets (financial, IT, reputation, business)
8	Non-respect of *anti-corruption* rules: bribery, illegal gratuities, etc.		
9	Uncontroled diffusion of confidential data		
10	Blocked site with "confinment"		
11	Hacking of IT system		
12	Competitive attack against the company's business interests (including reputation)		
13	Fraud problems after M&A or real estate operations		
14	Uncontrolled security costs related to projects		management of security
15	Decrease of Security budgets		

probability

Acceptability's frame of reference — area of priority management

	Bearable	Significant	Important	Major	gravity
Highly likely		15		9	
Likely	5	14	11 7	1 8 12	
Unlikely			13	3	
Highly unlikely			10	2 4 6	

14. How do you use the metric? What does it do for you? Does it guide your security decision-making?

The most important use is to prove to the CEO and to the Chairman that it is possible to pilot security like all other the processes in the company and obtain a return on investment—to employ security in line with the company's overall financial approach.

15. Can you share specifics—for example, specific measurements over time, specific security changes you made in response to the metric, and whether those changes had the desired effect?

Shared above.

Scoring and Comments from Reviewers

Based on the Security Metrics Evaluation Tool (Security MET)

Metric 10	Researcher	Expert 1	Expert 2	
Criterion	**Score**	**Score**	**Score**	**Average**
1. Reliability	4	4	3	3.67
2. Validity	3	5	3	3.67
3. Generalizability	4	5	3	4.00
Technical Total	**11**	**14**	**9**	**11.33**
4. Cost	3	4	5	4.00
5. Timeliness	4	5	3	4.00
6. Manipulation	4	3	3	3.33
Operational (Security) Total	**11**	**12**	**11**	**11.33**
7. Return on Security Investment	5	5	5	5.00
8. Organizational Relevance	5	5	5	5.00
9. Communication	5	5	5	5.00
Strategic (Corporate) Total	**15**	**15**	**15**	**15.00**
TOTAL ACROSS CRITERIA	**37**	**41**	**35**	**37.67**

Expert comments: The metric speaks to the hearts and minds of executives by focusing on money. This metric addresses the areas of risk, focuses security on areas that are important to the firm, shows the impact of security against sales to determine the effectiveness of the program, and, most importantly, shows that security aids in revenue generation by keeping loss well below projected cost. One challenge is that collecting timely data on losses and damages can be difficult. In presenting this metric, it could be useful to add a graphic that breaks down the four targeted areas of security by cost of countermeasures in each area against the impact to determine if spending is allocated optimally. Such information might aid in making the business case for more security in one area or another.

11. Operations Downtime Reduction Metric

1. **Respondent title**

   Head of Security Strategy, Planning, and Capability

2. **Organization's location, field/industry, number of employees, number of sites, annual revenue (or other measure of size)**

   Africa; energy/oil; part of worldwide company with 87,000 employees; $467 billion revenue

3. **Description of metric (what are you measuring, and in general why?)**

   We take several measures regarding security's impact on core corporate activities. For example:

   - security-related downtime during crude loading and offtake at the terminals (goal <5 percent)

   - amount of planned rig NPT (non-production time) due to security issues versus actual amount of NPT due to security issues (goal <5 percent of total rig availability time)

   - delays due to crude theft and asset vandalism (goal <10 percent)

4. **How long has the metric been used at the organization?**

   Two years.

5. **How reliable is the data you collect for the metric? Please explain.**

   The data is highly reliable as there are focal points for the collection of data. Some of the data comes from security and some from production staff.

6. **How do you ensure that the conclusions you draw from your metric are valid? Please explain.**

   Playing back the metrics on a monthly basis shows the trend and it's easy to see how things are playing out. When things get out of balance, we can quickly implement more controls or reviews.

7. **Would your metric be useful to other organizations? In other words, is it generalizable?**

   Some can be generalized, while others are specific to the oil and gas business.

8. **What is the cost of developing and administering your metric? This includes monetary and non-monetary costs associated with metric development and administration, as well as any negative consequences associated with collecting the data or using the metric (for example, data collection takes a lot of staff time or offends employees).**

   There are no additional costs. These metrics were developed in-house. The staff members responsible for administering the metrics are on the company payroll with this included in their job description.

9. **Can the data for your metric be collected in a timely fashion—so it is relevant for decision-making?**

   Yes.

10. **Could people fake the metric data if they wanted to? Is there any incentive for them to do so?**

   Not really. As these metrics are shared and analyzed, the figures can be challenged.

11. **Can your metric be used to demonstrate a return on security investment?**

   Yes. The metrics are directly linked to corporate efficiency and profitability. Our metrics help us reduce operations downtime.

12. **Is the metric aligned with your organization's goals, mission, objectives, assets, or risks? How?**

   Yes. These metrics are derived from the business objectives and focus area for the business.

13. **Are your metric and metric results easy to explain to others—especially to senior management?**

   Yes. We share results with senior management quarterly and with other members of the leadership team monthly.

14. **How do you use the metric? What does it do for you? Does it guide your security decision-making?**

   Our metrics guide security decisions by showing us when and where security incidents are getting out of the expected range.

15. **Can you share specifics—for example, specific measurements over time, specific security changes you made in response to the metric, and whether those changes had the desired effect?**

   We do change security arrangements based on the data, but we cannot share the details.

Scoring and Comments from Reviewers

Based on the Security Metrics Evaluation Tool (Security MET)

Metric 11	Researcher	Expert 1	Expert 2	
Criterion	Score	Score	Score	Average
1. Reliability	4	4	2	3.33
2. Validity	4	4	3	3.67
3. Generalizability	3	4	2	3.00
Technical Total	**11**	**12**	**7**	**10.00**
4. Cost	3	5	5	4.33
5. Timeliness	4	3	3	3.33
6. Manipulation	4	2	3	3.00
Operational (Security) Total	**11**	**10**	**11**	**10.67**
7. Return on Security Investment	5	5	3	4.33
8. Organizational Relevance	5	5	4	4.67
9. Communication	5	3	5	4.33
Strategic (Corporate) Total	**15**	**13**	**12**	**13.33**
TOTAL ACROSS CRITERIA	**37**	**35**	**30**	**34.00**

Expert comments: This metric focuses on impact, risk reduction, cost, and ROI. It is unclear whether the data is susceptible to manipulation. The metric appears to be shared regularly with varying levels of management, who would likely be very interested in reducing delays and downtime, the subjects of this metric.

12. Due Diligence Metric

1. **Respondent title**

   Chief Security Officer

2. **Organization's location, field/industry, number of employees, number of sites, annual revenue (or other measure of size)**

   Northeastern United States; finance/investment brokerage; 41,000 employees in offices mostly throughout the United States but also in other countries; $2.3 billion operating income

3. **Description of metric (what are you measuring, and in general why?)**

   We have created a multi-point metric to study the execution of due diligence investigations of our vendors (the companies we do business with). We measure:

   - cycle time (how long it takes us to complete our investigation)

   - various elements of our findings (specific types of derogatory findings)

   - success rate of our vendors (in passing our due diligence investigation)

4. **How long has the metric been used at the organization?**

   Approximately five years.

5. **How reliable is the data you collect for the metric? Please explain.**

   No concerns about reliability.

6. **How do you ensure that the conclusions you draw from your metric are valid? Please explain.**

   The benefits of the metric seem self-evident: fast investigations, quicker opportunity to start business activities, less chance of doing business with unsuitable partners, etc. However, we have not specifically validated the metrics through research.

7. **Would your metric be useful to other organizations? In other words, is it generalizable?**

   Yes.

8. **What is the cost of developing and administering your metric? This includes monetary and non-monetary costs associated with metric development and administration, as well as any negative consequences associated with collecting the data or using the metric (for example, data collection takes a lot of staff time or offends employees).**

   There is some cost. We have staff members dedicated to collecting the data for these metrics.

9. **Can the data for your metric be collected in a timely fashion—so it is relevant for decision-making?**

It is timely. We collect the data on an ongoing basis and report it quarterly to business heads.

10. **Could people fake the metric data if they wanted to? Is there any incentive for them to do so?**

The data seems true and accurate, though it is not 100 percent automated. Faking the data would not be impossible, but it would be hard and would not benefit anyone greatly.

11. **Can your metric be used to demonstrate a return on security investment?**

We can estimate our costs of conducting due diligence investigations, but it is hard to measure the benefit of avoiding business relations with shady companies. The losses we prevent could be very high, but we have not yet figured out how to demonstrate a clear, quantitative ROI with this metric.

12. **Is the metric aligned with your organization's goals, mission, objectives, assets, or risks? How?**

This metric directly helps our company reduce its likelihood of doing business with bad partners—companies that might be unreliable in their dealings with us or that might bring a stain to our company's reputation. Thus, it is aligned with the corporate goal of reducing risk (from unsuitable partners) and maximizing gain (by working with trustworthy partners).

13. **Are your metric and metric results easy to explain to others—especially to senior management?**

The corporation includes several distinct businesses. We report quarterly to each business head. We provide a dashboard of only the most important security metrics. We limit our presentation to 5 minutes.

We are trying to count the cost of security per employee. We would like to be able to speak the language of the CFO. I would like to calculate security cost per employee and share that figure so that it can become a benchmark in its specific industry. Other industries could do the same.

14. **How do you use the metric? What does it do for you? Does it guide your security decision-making?**

We mainly use the metric to show business heads that we are not slowing them down. The metric shows that we are protecting the company from unsuitable business partners while keeping to an announced, short cycle time in our due diligence investigations.

The way in which it may guide our decision-making is that we would like to find the optimal target time for these due diligence investigations. A shorter completion time is better than a longer completion time, yet reducing completion time (e.g., by hiring more investigators) may cost more than it is worth. We would like to find the sweet spot: the smallest number of days at which the benefit still outweighs the cost.

15. Can you share specifics—for example, specific measurements over time, specific security changes you made in response to the metric, and whether those changes had the desired effect?

Improved use of metrics is the path for us. It will be a concentration next year.

Scoring and Comments from Reviewers

Based on the Security Metrics Evaluation Tool (Security MET)

Metric 12	Researchers	Expert 1	Expert 2	
Criterion	**Score**	**Score**	**Score**	**Average**
1. Reliability	5	2	4	3.67
2. Validity	4	2	3	3.00
3. Generalizability	4	3	5	4.00
Technical Total	**13**	**7**	**12**	**10.67**
4. Cost	3	1	4	2.67
5. Timeliness	4	3	2	3.00
6. Manipulation	4	3	4	3.67
Operational (Security) Total	**11**	**7**	**10**	**9.33**
7. Return on Security Investment	3	2	3	2.67
8. Organizational Relevance	5	3	4	4.00
9. Communication	4	3	5	4.00
Strategic (Corporate) Total	**12**	**8**	**12**	**10.67**
TOTAL ACROSS CRITERIA	**36**	**22**	**34**	**30.67**

Expert comments: The organization using the due diligence metric is attempting to determine the best methods for increasing enterprise security, while balancing return on investment and validity. The metric's general applicability across different settings, organizations, and circumstances enhances the metric's overall utility. To improve the metric, the organization should invest in increasing its analytical capabilities to draw quantifiable correlations between identified "unstable partners" and established security protocols. The metric has been collected consistently over several years. Quarterly reports to senior management may not be frequent enough.

13. Shortage/Shrinkage Metric

1. **Respondent title**

   Vice President, Loss Prevention

2. **Organization's location, field/industry, number of employees, number of sites, annual revenue (or other measure of size)**

   Headquartered in western United States; 3,400 retail clothing stores worldwide; 136,000 employees; net sales approximately $16 billion

3. **Description of metric (what are you measuring, and in general why?)**

   First, we contribute to the corporation's calculation of shortage or shrinkage, that is, the difference between what our systems say we should have and our actual inventory. The metric is primarily calculated by the inventory control department. Shortage is a meta-metric or the ultimate metric, as it is the culmination of many different measures, such as losses in stores, in the supply chain, in transit, and from system problems that cause inaccurate counting.

   Second, we use the shortage metric to:

   - make the case for investment in security technologies,

   - test the effectiveness of that investment, and then

   - make the case for more investment in the proven-effective technologies.

   See question 15 below for a description of a specific use of this metric.

4. **How long has the metric been used at the organization?**

   Years.

5. **How reliable is the data you collect for the metric? Please explain.**

   The data is good. External theft is reported by loss prevention staff who perform apprehensions and find evidence of loss, such as electronic article surveillance tags that have been removed from products and left in the store. We also get reports of losses from store video. For internal losses, we perform investigations and make our own counts of losses.

6. **How do you ensure that the conclusions you draw from your metric are valid? Please explain.**

   The interplay between some of our activities and shortage reduction can be hard to pin down. For example, if our number of internal theft investigations is up, that could be a good sign, showing that we are becoming aware of more internal thefts and taking action. On the other hand, it could be a bad sign, showing that some aspect of a store's culture or systems is allowing internal theft to occur in the first place.

   However, by using the overall shortage metric, especially after making a clear change like adding security cameras, we can tell fairly confidently that our intervention made a difference.

7. **Would your metric be useful to other organizations? In other words, is it generalizable?**

   Yes. It is in widespread use in the retail industry.

8. **What is the cost of developing and administering your metric? This includes monetary and non-monetary costs associated with metric development and administration, as well as any negative consequences associated with collecting the data or using the metric (for example, data collection takes a lot of staff time or offends employees).**

   The inventory control department does much of the data collection. The work is happening anyway; creating the metric is not an add-on task.

9. **Can the data for your metric be collected in a timely fashion—so it is relevant for decision-making?**

   The data is collected on an ongoing basis. We can study it for feedback to judge the effectiveness of our interventions.

10. **Could people fake the metric data if they wanted to? Is there any incentive for them to do so?**

    Some data elements of the shortage metric are fully reliable, while others are in a gray area, such as the distinction between actual losses due to theft and apparent losses due to accounting or inventory errors.

11. **Can your metric be used to demonstrate a return on security investment?**

    There is a clear link between reducing shrinkage and saving money. Our metrics demonstrate that the investment in security technology led to reduced losses. We have found that if shortage goes up, senior management is willing to allocate resources to help us determine the cause and implement solutions.

12. **Is the metric aligned with your organization's goals, mission, objectives, assets, or risks? How?**

    The shortage number is a company-wide metric. It affects profit and loss for every store and for the corporation. Senior leadership is concerned because shortage hurts profit. Retail companies accrue for shortage, meaning they plan or budget for a certain percentage of shortage in their profit and loss estimates. So I have to aim to do better than the accrual—to bring shortage in below the estimate. By doing so, I bring a benefit straight to the corporate bottom line.

13. **Are your metric and metric results easy to explain to others—especially to senior management?**

    Our presentation to management is clear-cut: what is the shortage number, and how did we contribute to keeping it low? We also summarize the dollar benefit that comes from our apprehensions and recoveries, but the main item senior management cares about is the ultimate metric: shortage.

14. How do you use the metric? What does it do for you? Does it guide your security decision-making?

See below.

15. Can you share specifics—for example, specific measurements over time, specific security changes you made in response to the metric, and whether those changes had the desired effect?

One example: we had many stores with no security cameras. We selected a subset of those stores based on known shortage numbers, obtained corporate funding to add cameras in those stores, and used ongoing metrics to demonstrate that shortage decreased in the stores where we added cameras. That evidence of shortage reduction led to further investment in security technology, so now we have cameras in 100 percent of our stores.

When analyzing this metric—shortage—it is very important to consider the causes of losses. If faulty accounting shows that we are losing a certain type of item, but we are not actually losing it, then the security measures we would put in place to reduce that loss would be a waste of resources. In other words, we would be spending money to solve a non-problem.

Scoring and Comments from Reviewers

Based on the Security Metrics Evaluation Tool (Security MET)

Metric 13	Researcher	Expert 1	Expert 2	
Criterion	Score	Score	Score	Average
1. Reliability	4	4	3	3.67
2. Validity	3	5	2	3.33
3. Generalizability	5	5	4	4.67
Technical Total	**12**	**14**	**9**	**11.67**
4. Cost	4	4	5	4.33
5. Timeliness	4	5	5	4.67
6. Manipulation	3	5	3	3.67
Operational (Security) Total	**11**	**14**	**13**	**12.67**
7. Return on Security Investment	4	5	3	4.00
8. Organizational Relevance	5	5	5	5.00
9. Communication	4	5	4	4.33
Strategic (Corporate) Total	**13**	**15**	**12**	**13.33**
TOTAL ACROSS CRITERIA	**36**	**43**	**34**	**37.67**

Expert comments: This type of metric is in widespread use throughout the retail industry. The validity and reliability of the data are difficult to gauge, as staff reporting and video surveillance are not perfect data sources. Still, through a meticulous and verifiable accounting process, this metric helps security inform the C-suite why security countermeasures should be implemented to reduce shortage. The direct linkage between identified shortages and lack of security measures makes a compelling case for the need for additional security. The metric does not necessarily identify the root cause of the shortage.

14. Phone Theft Metric

1. Respondent title

Vice President, Security

2. Organization's location, field/industry, number of employees, number of sites, annual revenue (or other measure of size)

Midwest United States; financial services/investments/mortgage broker; 9,400 employees

3. Description of metric (what are you measuring, and in general why?)

We track assaults on employees who work at our offices in the central business district of our city. It is part of our risk management effort and our effort to attract and retain workers.

Specifically, we have been tracking "Apple picking," which is the theft of mobile phones by criminals who grab the phones out of users' hands. At our office sites downtown, we were experiencing a severe rash of phone theft. Our employees were victimized on the sidewalks all around our offices. This was happening as they came to work, when they went outside for lunch, and when they left to go home.

See details in question 15.

4. How long has the metric been used at the organization?

Approximately two years.

5. How reliable is the data you collect for the metric? Please explain.

It is highly reliable. It is based on incident reports from victims (our employees), police reports (to which we have immediate access through a special relationship), and video surveillance (because we have cameras viewing all the areas around our buildings).

6. How do you ensure that the conclusions you draw from your metric are valid? Please explain.

The validity seems clear. We had reliable reports of theft, we took security action based on those reports, and now the problem is eliminated.

7. Would your metric be useful to other organizations? In other words, is it generalizable?

Yes, this metric—showing mobile phone theft trends changing as we changed security tactics—could be used in almost any organization.

8. **What is the cost of developing and administering your metric? This includes monetary and non-monetary costs associated with metric development and administration, as well as any negative consequences associated with collecting the data or using the metric (for example, data collection takes a lot of staff time or offends employees).**

   This metric does not cost any extra money. We are already tracking a range of security incidents. This is part of our general mission, not an add-on cost.

   We use RSA Archer software that addresses incident management, risk management, and compliance. It helps us track incidents and discern trends.

9. **Can the data for your metric be collected in a timely fashion—so it is relevant for decision-making?**

   The data tends to be very up-to-date, as people generally report these victimizations promptly.

10. **Could people fake the metric data if they wanted to? Is there any incentive for them to do so?**

    A person could file a false report with the security department or with city police, but our investigation of the reported theft might show (through video) that the claimed incident did not take place. Also, there is little incentive to file a false report.

11. **Can your metric be used to demonstrate a return on security investment?**

    This metric is important and is valued by the company because it works. The metric helps us keep employees safe and continue to attract new employees. Those missions are vital to the company, but the ROI would be hard to quantify.

12. **Is the metric aligned with your organization's goals, mission, objectives, assets, or risks? How?**

    It is perfectly aligned with our goal of attracting, protecting, and retaining talent at our office locations in a city that experiences a high rate of crime. The company's risk management department pays close attention to this metric and related metrics.

13. **Are your metric and metric results easy to explain to others—especially to senior management?**

    I report our metric and related data to senior management every quarter. The purpose is to show the value of the security program. I present the data in summary form in a PowerPoint presentation. The key is to keep it simple and clear. I find it best to present a few short bullet points—the top-level information only, rather than complex charts and graphs. A dashboard containing multiple charts and graphs may be useful internally (within a security department), but for presentations to senior management, simpler is better.

14. How do you use the metric? What does it do for you? Does it guide your security decision-making?

See below.

15. Can you share specifics—for example, specific measurements over time, specific security changes you made in response to the metric, and whether those changes had the desired effect?
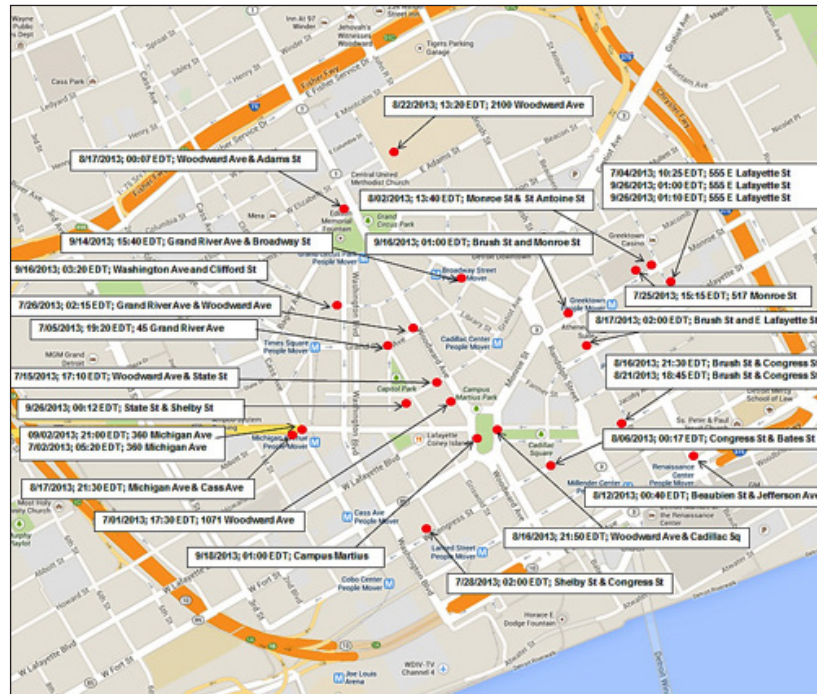
A few months ago, we had reached the point where we had 40 phone thefts in two months. In these incidents, a thief would snatch a mobile phone from one of our employees and run away. Our incident tracking process showed us how many thefts occurred, where exactly, and when. We were able to identify hot spots and times for phone theft and apply extra security measures at those places and times.

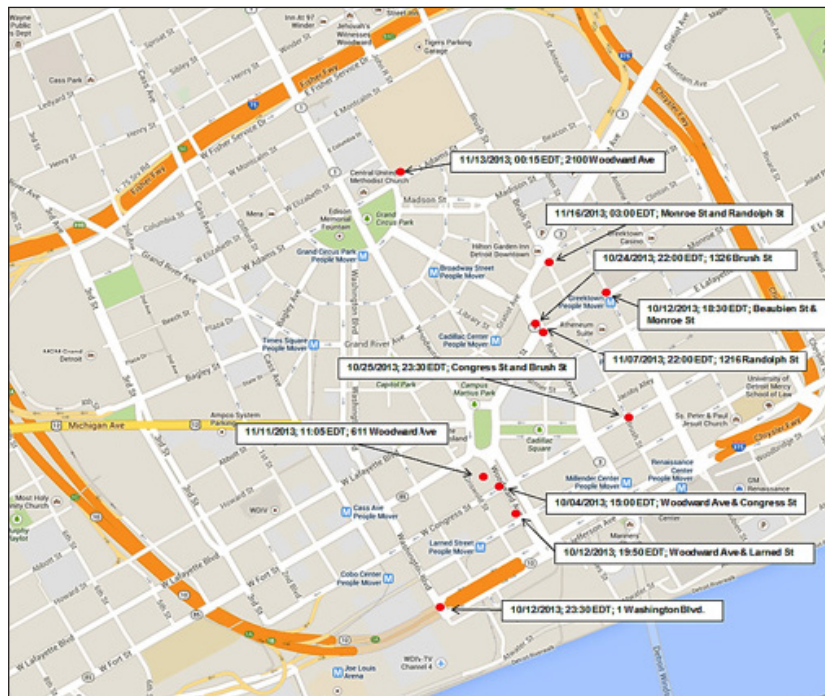These were our special measures:

- We installed more cameras in the hot spots.

- At the morning rush, lunchtime, and evening rush, we placed security officers outside our buildings instead of in the lobbies.

- We asked for, and received, increased police patrol at the hot spots. (We have a close relationship with local police, and our request was supported by detailed incident reports and video images.)

- We directed our officers to approach employees who looked vulnerable (not paying attention while talking on phones) and hand them special flyers with information on safe behavior (to avoid being victimized) and phone retrieval/locator apps that they can download to their phones.

- With our video images of "Apple picking" incidents, we created "be on the lookout" sheets and sent them to 30 local security directors and all our parking attendants.

- In concert with the local police, we investigated the thefts perpetrated against our employees. Some of the thieves were subsequently caught.

After taking these measures, we eliminated phone theft. After a height of 40 thefts in two months, we are now down to zero.

Third Quarter 2013:

Fourth Quarter 2013 (theft much reduced):

Scoring and Comments from Reviewers

Based on the Security Metrics Evaluation Tool (Security MET)

Metric 14	Researcher	Expert 1	Expert 2	
Criterion	Score	Score	Score	Average
1. Reliability	5	4	5	4.67
2. Validity	4	4	5	4.33
3. Generalizability	4	2	5	3.67
Technical Total	13	10	15	12.67
4. Cost	4	4	5	4.33
5. Timeliness	4	4	4	4.00
6. Manipulation	4	3	4	3.67
Operational (Security) Total	12	11	13	12.00
7. Return on Security Investment	2	4	5	3.67
8. Organizational Relevance	5	4	5	4.67
9. Communication	5	5	5	5.00
Strategic (Corporate) Total	12	13	15	13.33
TOTAL ACROSS CRITERIA	37	34	43	38.00

Expert comments: This metric served a useful purpose in quantifying a problematic threat and vulnerability and tracking the positive impacts that a multifaceted security countermeasure strategy had over time. The simplicity, reliability, and validity of the data led to readily understandable reporting to corporate leadership and a straightforward justification for additional security resources (where return on investment could clearly be seen). This example shows that a metric may be used for a short period and can be phased out once a specific problem has dissipated.

15. Security Inspection Findings Metric

1. **Respondent title**

   Senior Technical Advisor, Security Division

2. **Organization's location, field/industry, number of employees, number of sites, annual revenue (or other measure of size)**

   Government entity; very large; many sites.

3. **Description of metric (what are you measuring, and in general why?)**

   We collect three categories of metrics:

   - input process metrics (counting personnel and buildings that we must protect)

   - output metrics (counting tasks performed, such as security clearances)

   - outcome metrics (measuring the results of our work; the hardest type of metric to do well)

   Our Security Inspection Findings Metric is an outcome metric. We perform periodic inspections at our many facilities around the country to look for compliance with security rules. If we discover a violation (called a "finding"), such as an unlocked door or unsecured computer, we note it and make a recommendation or order for it to be corrected. Before we started keeping the Security Inspection Findings Metric, we would not always find out whether findings were corrected until we made our next periodic inspection, which could be a long time, meaning findings might go uncorrected for a year. Corrections were falling through the cracks. Now the person to whom the findings were reported must report to us how and when each finding is resolved, and our tracking methodology enables us to ensure that findings are resolved promptly. If they are not, we follow up with the site. There is no more falling through the cracks.

   So, the purpose of this metric is to ensure that findings are corrected in a reasonable period. Adhering to security guidelines is a clear and essential requirement for our organization, so correcting findings is essential to our organization's mission.

4. **How long has the metric been used at the organization?**

   Approximately 10 years.

5. **How reliable is the data you collect for the metric? Please explain.**

   The data is reliable. We collect it ourselves based on our own observations.

6. **How do you ensure that the conclusions you draw from your metric are valid? Please explain.**

   It is a straightforward proposition. If a greater percentage of findings is corrected, then we are experiencing better compliance with the security requirements our entity must meet.

7. **Would your metric be useful to other organizations? In other words, is it generalizable?**

It would be useful to any organization that tracks inspections.

8. **What is the cost of developing and administering your metric? This includes monetary and non-monetary costs associated with metric development and administration, as well as any negative consequences associated with collecting the data or using the metric (for example, data collection takes a lot of staff time or offends employees).**

Some parts of the data collection are automated, and other parts require manual tabulation. We tabulate the data monthly. The metric requires about one day of labor per month.

9. **Can the data for your metric be collected in a timely fashion—so it is relevant for decision-making?**

We collect and tabulate the data monthly, which is frequent enough for our decision-making purposes.

10. **Could people fake the metric data if they wanted to? Is there any incentive for them to do so?**

We collect the initial data ourselves (the findings that arise from our inspections), and we track corrections of those findings. Someone could falsely report that a finding was corrected, but we would find out at the next inspection.

11. **Can your metric be used to demonstrate a return on security investment?**

The actual financial return on investment cannot be calculated in our entity. However, the value of the metric is clear to senior management. This metric enables us, on a tight budget, to justify the expense of our inspections. We show our value by measuring our increasing success in ensuring that findings are corrected promptly and not allowed to fall through the cracks.

12. **Is the metric aligned with your organization's goals, mission, objectives, assets, or risks? How?**

The metric is tied directly to the organization's strategic and business plans, which include security goals. The metric shows whether we are successfully executing those plans.

13. **Are your metric and metric results easy to explain to others—especially to senior management?**

The metric is easy to explain to senior management. Over time, we have learned that less is more. We asked senior management what they really wanted to see. They said they cared about only seven particular items from our 30-page report. Now we give a short slide presentation about our metrics—no more than 10 slides. I am working to create an even simpler dashboard for senior management.

14. **How do you use the metric? What does it do for you? Does it guide your security decision-making?**

The metric results in increased adherence to decisions that have already been made—that is, the security rules that sites must follow. The metric partly guides decision-making by senior management by showing them that our inspections and follow-up activity are resulting in faster and surer resolution of security deficiencies.

15. **Can you share specifics—for example, specific measurements over time, specific security changes you made in response to the metric, and whether those changes had the desired effect?**

With this metric, which makes findings follow-up possible, we have been able to significantly increase the percentage of findings that are resolved promptly. This is an important benefit to the organization.

Scoring and Comments from Reviewers

Based on the Security Metrics Evaluation Tool (Security MET)

Metric 15	Researcher	Expert 1	Expert 2	
Criterion	Score	Score	Score	Average
1. Reliability	4	3	3	3.33
2. Validity	5	3	3	3.67
3. Generalizability	4	4	4	4.00
Technical Total	**13**	**10**	**10**	**11.00**
4. Cost	4	3	5	4.00
5. Timeliness	4	3	3	3.33
6. Manipulation	4	2	3	3.00
Operational (Security) Total	**12**	**8**	**11**	**10.33**
7. Return on Security Investment	2	3	3	2.67
8. Organizational Relevance	5	4	3	4.00
9. Communication	5	3	3	3.67
Strategic (Corporate) Total	**12**	**10**	**9**	**10.33**
TOTAL ACROSS CRITERIA	37	28	30	31.67

Expert comments: Quantifying and demonstrating ROI from security oversight functions, such as surveys, audits, assessments, inspections, and red/blue team operations, is often challenging. This example illustrates an innovative approach by not only tabulating instances of vulnerabilities detected and instances of regulatory noncompliance, but also documenting corrective actions taken and completed as a result of the inspection process. This metric should be of high interest to corporate leadership.

Data quality could be a challenge. Inspectors have varying interpretations of the rules, and the use of infrequent inspections affects the timeliness of the data. The metric might be even more useful for senior management if it reported how many high-, medium-, and low-level risks were mitigated.

16. Infringing Website Compliance Metric

1. **Respondent title**

   Senior Director, Corporate Security

2. **Organization's location, field/industry, number of employees, number of sites, annual revenue (or other measure of size)**

   Northeastern United States; pharmaceuticals; $1.4 billion revenue; four main sites

3. **Description of metric (what are you measuring, and in general why?)**

   Thousands of websites claim to offer our products (brand-name prescription drugs) for sale without a prescription. These are highly regulated Schedule 2 drugs. Offering our products in this manner is a trademark infringement. (And actually selling the drugs in this manner is a felony.)

   Suppressing these crooked websites is important because they endanger public health (by providing real or fake pills illegally), misuse our intellectual property, and harm our corporate brand. Most of the sites are spurious, existing to facilitate credit card fraud and identity theft.

   We send cease-and-desist letters to owners of such sites, demanding that the sites be taken down because they infringe our trademark. Our metric is the percentage of website owners or Internet service providers who comply with these cease-and-desist letters.

   Measuring the compliance rate helps us measure our effectiveness in taking the sites down.

4. **How long has the metric been used at the organization?**

   Three and a half years.

5. **How reliable is the data you collect for the metric? Please explain.**

   It is very reliable. Cease-and-desist letters are simple to count, as are taken-down websites.

6. **How do you ensure that the conclusions you draw from your metric are valid? Please explain.**

   On one level, if our compliance rate rises, that is a clear sign that our cease-and-desist letters are more effective in taking down infringing sites.

   As for drawing other conclusions from the metric, we use our data to try to influence Internet policy (through ICANN, the Internet Corporation for Assigned Names and Numbers) and law enforcement efforts. We do not draw conclusions that the data cannot support—in particular, we cannot say that a high compliance rate necessarily results in fewer infringing websites over time. We draw what seems to be a valid conclusion: that a higher compliance rate is better than a lower compliance rate if we wish to shut down infringing sites.

7. **Would your metric be useful to other organizations? In other words, is it generalizable?**

   Any organization with products or intellectual property misused online could benefit from establishing a program of sending cease-and-desist letters to infringers and tracking the effectiveness of those letters. The work can be done in-house or with a vendor.

8. **What is the cost of developing and administering your metric? This includes monetary and non-monetary costs associated with metric development and administration, as well as any negative consequences associated with collecting the data or using the metric (for example, data collection takes a lot of staff time or offends employees).**

   We use a vendor to identify the sites, send cease-and-desist letters, and track whether the sites are taken down. There is a cost to using the vendor. It is important to use a high-quality vendor for this task, and the vendor is not cheap. It would take two to three full-time people on our staff to do what the vendor is doing for approximately the cost of one person.

   However, the actual metric—the compliance rate—does not have a marginal cost above the main work that the vendor is doing. The metric is a straightforward measurement that would need to be taken anyway.

9. **Can the data for your metric be collected in a timely fashion—so it is relevant for decision-making?**

   Yes. The data is collected quickly and automatically.

10. **Could people fake the metric data if they wanted to? Is there any incentive for them to do so?**

    Our vendor could attempt to fake the data, in order to appear more successful, but the numbers are easy to verify.

11. **Can your metric be used to demonstrate a return on security investment?**

    The ROI is there, but it is not easy to measure. The investment is mainly the cost of the vendor we use. The vendor's work has a known cost, but the return—brand protection, intellectual property protection, public health protection, identity theft, and credit card fraud prevention—is hard to quantify.

    Sometimes the program is a hard sell, even though the costs are visible, the metric is clear, and the benefits are important. Still, this effort continues to be funded even in a cost-cutting era.

12. **Is the metric aligned with your organization's goals, mission, objectives, assets, or risks? How?**

    I believe 75 percent of a company's assets are non-physical. Brand protection and protection of intellectual property, which our metric supports, are absolutely vital to the corporation's goals. Our compliance metric is an important part of risk management.

13. **Are your metric and metric results easy to explain to others—especially to senior management?**

The metric is straightforward: what percentage of websites were taken down after their owners or ISPs received our cease-and-desist letters.

14. **How do you use the metric? What does it do for you? Does it guide your security decision-making?**

See below.

15. **Can you share specifics—for example, specific measurements over time, specific security changes you made in response to the metric, and whether those changes had the desired effect?**

Things move fast on the Internet. We use a vendor called MarkMonitor, which searches the Web for infringing sites. After the automated, algorithm-based system finds a possibly infringing site, the site is quickly investigated (within three to four days) to determine whether it is in fact infringing. If so, a cease-and-desist letter is sent to the site owner. A week later, if the site is still up, similar letters are sent to the Internet service provider that hosts the site and to the domain name registrar. Noncompliance results in further measures from us.

Over the last three and a half years, by using this automated approach we have increased compliance from 84 percent to 98 percent. That means 98 percent of the sites to which we send cease-and-desist letters actually get taken down.

Over the course of a month, we generally have a rolling average of 50 problematic sites. Our metric does not provide a silver bullet to stop the problem; we cannot identify and stop every offender on the Internet. Rather, our orderly, consistent approach to suppressing these sites helps us keep the problem to a manageable level.

The metric guides our decision-making by telling us whether our cease-and-desist letters continue to be effective. The metric also guides public policy, Internet policy (ICANN), and law enforcement/prosecution activities when we share our findings with outside organizations.

Scoring and Comments from Reviewers

Based on the Security Metrics Evaluation Tool (Security MET)

Metric 16	Researcher	Expert 1	Expert 2	
Criterion	Score	Score	Score	Average
1. Reliability	5	5	3	4.33
2. Validity	4	5	2	3.67
3. Generalizability	4	5	1	3.33
Technical Total	**13**	**15**	**6**	**11.33**
4. Cost	2	4	3	3.00
5. Timeliness	5	5	3	4.33
6. Manipulation	5	5	2	4.00
Operational (Security) Total	**12**	**14**	**8**	**11.33**
7. Return on Security Investment	3	4	2	3.00
8. Organizational Relevance	5	5	3	4.33
9. Communication	5	5	2	4.00
Strategic (Corporate) Total	**13**	**14**	**7**	**11.33**
TOTAL ACROSS CRITERIA	**38**	**43**	**21**	**34.00**

Expert comments: This metric shows that compliance with cease-and-desist requests has increased substantially over time. The metric is not able to determine the impact on the total number of violating sites, the number of re-established infringing websites, or any possible deterrent benefits. Still, the metric justifies the continuance of cease-and-desist letters to make at least a marginal difference and thus is worth the modest cost of sustaining it.

Appendix C: Literature Review

Executive Summary

Metrics drive business decisions and behavior. They influence process assessment and controls, business policies, collaboration for enterprise-wide benefits, business investment decisions, and strategic and profit center alignment. Security metrics are vital, but the field offers few tested metrics and benchmarks (Guidelines and Metrics Working Group, ASIS Defense and Intelligence Council, 2012).

This literature review will help security professionals discover and understand metrics that are currently in use, present metrics to executive management in a persuasive manner, and evaluate existing metrics. Existing security metrics can be categorized based on security type (Guidelines and Metrics Working Group, ASIS Defense and Intelligence Council, 2012), business function ("CIS consensus information security metrics," n.d.), degree of automation (McIIravey & Ohlhausen, 2012), etc. The literature also presents aids in communication to best present these metrics to management, including benchmarks (GIA, 2010). In addition, general tips are provided in the literature on how to evaluate the effectiveness of a measure, including demonstrating return on investment (Gauging security ROI, 2007).

The present literature review identifies a gap regarding the existence and evaluation of statistically sound metrics. Explicitly defined metric criteria, evidence needed to document that these criteria were met, and example metrics that meet these criteria do not yet exist within the security literature. Valid and reliable metrics are vital in ensuring that accurate conclusions are drawn from data and the right information is communicated; this would ultimately drive management to fully comprehend the importance and value of security and security metrics. The development of the Security Metrics Evaluation Tool (Security MET) should address this crucial gap.

I. Introduction

Metrics drive business decisions and behavior. They enable process assessment and controls, drive business policies, influence collaboration for enterprise-wide benefits, drive business investment decisions, and influence strategic and profit center alignment. Security metrics are vital, but the field offers few tested metrics or benchmarks (Guidelines and Metrics Working Group, ASIS Defense and Intelligence Council, 2012). With a significant rise in the availability and use of big data (i.e., datasets that are so voluminous that the ability to structure, process, and comprehend the data is arduous), it is imperative that organizations select the right metrics. For example:

> "CSC…predicts that by 2020, we will see a 4,300 percent increase in the rate of annual data generation" (Van Till, 2013, para. 3).

Harnessing big data through metrics will be essential in helping organizations remain competitive (Bewley, 2013; Kiron, Shockley, Kruschwitz, Finch, & Haydock, 2011).

A. Evolution of Security Metrics

Historically, there has been a disconnect between security programs and the core businesses they serve. However, the risk environment has dramatically changed within the last 30 years, in part due to new avenues in technology (Campbell, 2006). Security programs must now gauge their effectiveness in terms of risk mitigation and do so in a way that speaks to senior executives. Metrics are a vital tool for this gauge, and as such, the perceived value of metrics is on the rise (Campbell, 2007).

For example, in "Make Better Decisions," Davenport (2009) describes the benefits of metrics. Davenport uses the term "analytics" to describe decision-making driven by quantitative analysis and data. When a company uses metrics or analytics, the decisions made are more likely to be the right ones, as these decisions are grounded in the scientific method.

Security metrics support the value proposition of an organization's security operation. However, the focus is more on counting events than creating meaningful, risk-based metrics (Hayes & Kotwica, 2012). The optimization of metric value is not widely understood. In their Harvard Business Review article, Davenport and Harris (2010) report results from their study of 400 companies in 35 countries and 19 industry sectors. They write, "Those who view [metrics] as just reporting on past performance don't understand the full scope and value of analytics" (Davenport & Harris, 2010, p.1).

B. Definition of Security Metrics

The adjacent box contains an old definition of security metrics from Carnegie Mellon University (1995):

This definition can be broadened to include the protection of people, property, and information. Security metrics are a crucial aspect of risk management (Azuwa, Ahmad, Sahib, & Shamsuddin, 2012). In the information security field, researchers have defined metric in numerous ways (Azuwa et al., 2012):

> "Metrics are quantifiable measurements of some aspect of a system or enterprise…. Security metrics focus on the actions (and results of those actions) that organizations take to reduce and manage the risks of loss of reputation, theft of information or money, and business discontinuities that arise when security defenses are breached" (Carnegie Mellon University, 1995, para.1-2).

- a measurement that is compared to a scale or benchmark to produce a meaningful result
- a quantitative and objective basis for security assurance, comparing two or more measurements taken over time with a predetermined baseline
- an indicator, not an absolute value with respect to an external scale
- a measurement standard that can be quantified and reviewed to meet security objectives, facilitate relevant actions for improvement, and aid decision making and compliance with security standards

The term *metrics* is sometimes used interchangeably with measurements, analytics, and performance metrics throughout the security literature. To aid in clear and consistent communication, only the term *metrics* is used throughout this review.

C. Purpose of This Literature Review

The purpose of this review is to synthesize literature surrounding existing metrics, communicating metrics, and evaluating metrics. This will serve as the first step in guiding security professionals to develop metrics that meet measurement standards, present metrics to executive management in a persuasive manner, and evaluate existing metrics. Metrics allow organizations to hold individuals accountable for specified results and goals, and are a vehicle through which security programs can demonstrate their measurable impact on an organization's strategic, organizational, financial, and operational risks and profits (Campbell, 2007). As such, an integration of metrics literature is essential for furthering the understanding of what metrics exist, how to effectively communicate metrics, and what makes a good metric.

It is important to note that the metrics discussed, and principles of communicating and evaluating metrics, are applicable across all domains of security. Below is a list of the ASIS International Councils to illustrate the widespread applicability of this literature review to the broad field of security:

- Academic and Training Programs Council
- Banking and Financial Services Council
- Commercial Real Estate Council
- Crime/loss Prevention Council
- Crisis Management and Business Continuity Council
- Cultural Properties Council
- Defense and Intelligence Council
- Economic Crime Council
- Fire and Life Safety Council
- Food Defense and Agriculture Security Council
- Gaming and Wagering Protection Council
- Global Terrorism, Political Instability and International Crime Council
- Healthcare Security Council
- Hospitality, Entertainment and Tourism Security Council
- Information Asset Protection & Pre-employment Screening Council
- Information Technology Security Council
- Investigations Council
- Law Enforcement Liaison Council
- Leadership and Management Practices Council
- Military Liaison Council
- Petrochemical, Chemical and Extractive Industries Security Council
- Pharmaceutical Security Council

- Physical Security Council
- Retail Loss Prevention Council
- School Safety and Security Council
- Security Architecture and Engineering Council
- Security Services Council
- Supply Chain and Transportation Security Council
- Utilities Security Council
- Women In Security Ad-hoc Council

II. Existing Security Metrics

There have been multiple efforts aimed at examining existing security metrics. Perhaps the most thorough treatment of the topic to date is that by Campbell (2007). Existing security metrics can be categorized based on security type (Guidelines and Metrics Working Group, ASIS Defense and Intelligence Council, 2012), business function ("CIS consensus information security metrics," n.d.), degree of automation (McIIravey & Ohlhausen, 2012), etc.

> **Existing Security Metrics Outline:**
>
> A. Campbell's 2007 Metric Review
>
> B. Metrics by Security Type
>
> C. Metrics by Business Function
>
> D. Return-on-Investment Metrics
>
> E. Metrics – Incident Management Software
>
> F. Existing Metrics – Concluding Remarks

Examples of metric categories and corresponding metrics that will be discussed include:

- Baseline performance metrics, such as emergency service response time (Campbell, 2007)
- Physical security metrics, such as the number of persons who voluntarily showed identification badges versus those who did not (Scaglione, 2012)
- Financial metrics, such as the security cost per employee (McIIravey & Ohlhausen, 2012)
- Return-on-investment metrics, such as decline in amount of network downtime (Gauging security ROI, 2007)
- Metrics managed via incident management software, such as the number of policy violations (Gips, 2004)

A. Campell's 2007 Metric Review

In his review, Campbell (2007) provides a description of numerous types of metrics and discusses many of the issues pertaining to their use in organizations. Key performance indicators (KPIs) are one type of metric; KPIs are established by identifying a desired performance level and assessing the progression, or lack thereof, toward that level (Campbell, 2007). Examples of KPIs include employee and customer satisfaction surveys, the number of shipped goods that arrive to their destination intact, and the number of information security events that occur within a year (Mayor, 2006; Pironti, 2007).

Risk analyses are another category of metric. This could involve measuring assets in terms of cost of loss or loss events, or conducting a cost-benefit analysis (Campbell, 2007). Baseline performance metrics can also be valuable; emergency service response time would be an example of a baseline performance metric. Diagnostic metrics involve identifying the root causes of trends; for example, an organization might examine the causes of increased workplace violence incidents in a specific branch. Additional metric categories are listed below:

- Risk rating or ranking
- Threat assessment
- Vulnerability assessment
- Annualized loss expectancy

For a more comprehensive discussion of these metric types, see Campbell (2007).

B. Metrics by Security Type

Apart from the review conducted by Campbell (2007), security metrics are often categorized based on the type of security (human resources/personnel security, physical security, industrial security, information and cyber security, etc.) in which they are used. Human resources or personnel security addresses measurable issues including compliance, cost controls and efficiency, and continuous evaluation (Guidelines and Metrics Working Group, ASIS Defense and Intelligence Council, 2012). For example, a proposed metric for human resources security, in regard to employee changes/ terminations, can be found in the box below:

> "Percentage of user IDs belonging to people who have left the organization, separated into active (pending deactivation) and inactive (pending archival and deletion) categories" (ISO27k, 2007, p.4).

An additional metric for human resources security is the rate of turnover (i.e., staff retention; Campbell, 2012). The percentage of employees whose background checks yield negative findings is also a personnel security metric, as is the average time needed to conduct background checks (Getting started using performance metrics, 2005; How metrics can link security to the business, 2011; Wailgum, 2005).

Measureable events within industrial security include security reviews and workforce factors. Industrial security metrics might include the number of deficiencies reported; the number of classified contracts could also be useful (Guidelines and Metrics Working Group, ASIS Defense and Intelligence Council, 2012).

Physical security metrics can include measureable issues surrounding alarms, protective barriers, theft, etc. Garcia (2008, p. 8) writes:

> The performance measures for a PPS [physical protection system] function include probability of detection; probability of and time for alarm communication and assessment; frequency of nuisance alarms; time to defeat obstacles; probability of and time for accurate communication to the response floor; probability of response force deployment to adversary location; time to deploy to a location; and response force effectiveness after deployment.

These measures or metrics play an important role in a performance-based approach to meeting the objectives of a physical protection system (Garcia, 2008). They are also useful in vulnerability assessment. For example (Garcia, 2006, pp. 14-16):

> The goal of exterior sensor evaluation is to provide an estimate of sensor performance (P_D) against defined threats, along with supporting notes, pictures, and observations that support this estimate. This will help establish the baseline performance of the overall PPS and, if not acceptable, will provide opportunities for upgrade improvements. Factors that will cause performance degradation include nuisance alarm rate and ease of defeat of the sensor through bypass or spoofing….

> [In] this part of the VA [vulnerability assessment], an estimate of the probability of assessment (P_{As}) must be provided for use in the system analysis. This probability is a result of the combined effects of video image quality and resolution, speed of capture of images, proper installation and maintenance of all components, and integration of sensor detection zones with camera field-of-view coverage.

Another example of a physical security metric is the number of patients searched by emergency services at a hospital; the number of armed robberies at a specific store location and inventory shrinkage are additional examples (Health Resource Network, Inc., 2000; Wailgum, 2005). The number of door alarm annunciations is another physical security metric that is often implemented. This metric has been used to explore the cause of false alarms so that all alarms do not have to be treated as emergency security situations (Treece & Freadman, 2010). The number of persons who voluntarily show identification badges versus those who do not is another metric (Scaglione, 2012). In addition, the Transportation Security Administration is pursuing flier threat-level calculations, conducted by private data brokers, to determine whom to screen at security checks (Sternstein, 2013).

In establishing a metric to assess a given security function, security professionals are advised to ask the following questions (Kovacich & Halibozek, 2006):

- What specific data will be collected?
- How will the data be collected?
- When will the data be collected?
- Who will collect the data?
- Where (at what point in the function's process) will the data be collected?
- What will the data depict?
- How will it be communicated?
- In what form will it be displayed?

An important new treatment of physical security metrics is found in *The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard* (Interagency Security Committee, 2013). The Interagency Security Committee, chaired by the U.S. Department of Homeland Security, develops security standards and best practices for nonmilitary federal facilities in the United States. The standard recognizes security metrics as an important component of risk management. It states that, pursuant to Executive Order 12977, "the following policy is hereby established for the security

and protection of all buildings and facilities in the United States occupied by Federal employees for nonmilitary activities…:

- Federal departments and agencies shall assess and document the effectiveness of their physical security programs through performance measurement and testing;
- Performance measures shall be based on agency mission goals and objectives; and
- Performance results shall be linked to goals and objectives development, resource needs, and program management."

The standard addresses input or process measures, output measures, and outcome measures.

The security domain that has by far the greatest presence in the metrics literature is information and cyber security. International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 27001 is a widely used, best practice certification that outlines information technology security standard requirements surrounding the range of threats and vulnerabilities. The ISO/IEC 27001 standard mandates the measurement of information security as a requirement (Azuwa, Ahmad, Sahib, & Shamsuddin, 2012). One such requirement is shown in the accompanying box. In addition, the ISO/IEC 27002 standard dictates security techniques for managing information security (ISO/IEC, 2005b). These standards highlight the importance of information and cyber security, as well as related metrics.

> 4.2.3(c) "Measure the effectiveness of controls to verify that security requirements have been met" (ISO/IEC, 2005a, p.6).

Information and cyber security should focus on analyzing data in real-time; the results of the analyses should instantaneously trigger defensive action (Embracing big data can lead to greater security, 2013). Measurable issues within information security include inspection, incident management, change management, and classification measurement (Guidelines and Metrics Working Group, ASIS Defense and Intelligence Council, 2012; Rathbun, 2009). Other assessable information security controls include identification and authentication, audit and accountability, etc. (Azuwa, Ahmad, Sahib, & Shamsuddin, 2012). An example of an information security metric is the percentage of security incidents caused by improper access control configuration (Chew, Clay, Hash, Bartol & Brown, 2006; Wailgum, 2005). The loading time for the first webpage based on network lines is an additional metric for information security (Straub, Hoffman, Weber, & Steinfield, 2002). The numeric total of new viruses identified on the Internet is a metric of active security posture, an aspect of information security (Garigue & Stefaniu, 2003).

Additional information and cyber security metrics include:

- Viruses detected in user files (Ravenel, 2006)
- The percentage of information systems with annual testing focused on contingency planning (Whitman & Mattord, 2012)
- Balanced circuit security (Burns, Bystrov, Koelmans, & Yakolev, 2011)
- Interoperability problems associated with certification authorities and public key infrastructure (Casola, Mazzeo, Mazzocca, & Vittorini, 2007)
- Viruses/trojans received and internal incidents (Collins, 2004)

- Time needed to encrypt a sensitive document (Doinea & Pavel, 2010)
- Number of weak password breaches reported by employees in the past year (Aleem, Wakefield, & Button, 2013)

The literature on information and cyber security metrics is voluminous. Even so, all security domains (e.g., personnel, physical, industrial) remain in need of more, better-defined, and empirically tested metrics.

C. Metrics by Business Function

Metrics can also be organized by business function. For example, average time for change completion is a metric for configuration change management, and budget allocation for information security is a financial metric ("CIS consensus information security metrics," n.d.; Berinato, 2005). Additional financial metrics include the security cost per employee and annual security costs in relation to annual revenue (McIlravey & Ohlhausen, 2012). Average recovery time would fall into the incident management function. Patch compliance with policy and patch latency are both examples of patch management metrics. Scan coverage for vulnerabilities would be considered within the vulnerability management function ("CIS consensus information security metrics," n.d.; Berinato, 2005).

D. Return-on-Investment Metrics

In addition to business function, return on investment can serve as a framework for categorizing existing metrics. A Global Information Security Survey was conducted by *Information Week* and Accenture on more than 1,100 professionals in the field of business technology (Gauging security ROI, 2007). Below are the results to the question "How does your company measure the value of your security investments?"

- Fewer worker hours spent on security-related issues—43%
- Better protection of customer records—35%
- Decline in breaches—33%
- Decline in amount of network downtime—33%
- Improved protection of intellectual property—27%
- Better risk-management strategies—25%
- Reduction in incident-response time—24%
- We don't measure the value—24%

An interview- and literature-based report titled "Demonstrating the Value of Security" offers this finding:

> "An annual savings or cost avoidance of $9.2 million, 41 percent of the security budget, was gained in the first year since implementation of the new program. This savings reflects a number of changes to the security program, but the main change was the deployment of security personnel during higher-risk times. Before the use of the program, security personnel were used haphazardly, with no regard for actual risk levels. By deploying personnel only during peak risk times, the company saved over $9 million. It expects to retain a similar savings level in the years to come" (Vellani, 2004, p. 35).

One application of ROI is exemplified by the Cisco Cybercrime Return on Investment Matrix, which is used to predict successful cybercrime techniques (Cisco 2010 annual security report: Highlighting global security threats and trends, n.d.). Another application of ROI involves a retail chain implementing crime analysis software that captured the nature, time, location, and date of store crimes. Based on this data, a significant ROI was both achieved and measured:

> "The security function needs to collect metrics to highlight how it is adding value…. [W]ithout metrics it is not possible to show value in a form that business leaders will most clearly understand" (Gill, Burns-Howell, Keats, & Taylor, 2007).

E. Metrics – Incident Management Software

Some metrics are captured instantaneously through incident management software (IMS), such as the IMS used in emergency preparedness (McIIravey & Ohlhausen, 2012; Dallas county uses DHS grant to grab incident management software, 2008); the software can be configured based on business rules, and notifications can be set up based on specific rule violations (Huff, 2013). IMS from iViewsystems is currently being used at Hershey Entertainment & Resorts (HE&R) to manage security metrics, such as employee injuries, and to document and share data (Case study: Hershey Entertainment & Resorts, n.d.). Delta Air Lines uses Perspective from PPM 2000 to track compliance issues, accidents, medical emergencies, and financial crimes; the metrics then lead to policy recommendations both inside and outside the security department (McIIravey & Ohlhausen, 2012). Advanced data collection may also facilitate benchmarking and a more standardized approach to security return on investment.

In the IT world, enterprise rights management (ERM) software has grown in usage over the past several years; this technology can be used to remove employee access to networks and thus mitigate employees that are leaving an organization from accessing proprietary information at a later point in time (Wagley, 2007). InSight Security Manager software can be used to identify anomalies, such as the number of policy violations (Gips, 2004).

F. Existing Metrics – Concluding Remarks

This section explored the status of existing security metrics. The most thorough metric review to date was done by Campbell (2007); in his summary, Campbell describes metrics as falling into numerous categories, such as key performance indicators, risk analyses, and diagnostic measures. Security metrics have also been categorized based on security type, including human resources/personnel security, physical security, industrial security, information and cyber security, etc. (Guidelines and Metrics Working Group, ASIS Defense and Intelligence Council, 2012). Business function is an additional framework used to explore different metrics, such as metrics that fall within the financial or risk management functions ("CIS consensus information security metrics," n.d.). Metrics can also be explored based on their degree of automation, such as metrics obtained from an incident management system (McIIravey & Ohlhausen, 2012). Unfortunately, many metrics are presented only at a conceptual level; it is difficult to ascertain what exactly is being measured and how this measurement is obtained. As such, duplicating the measures presented above would likely not be a straightforward process. In addition, the current focus of security metrics remains more on summative indicators rather than meaningful, risk-based metrics (Hayes & Kotwica, 2012).

Grounding metrics in risk assessment, key business goals and objectives, and the principles of measurement is crucial in capitalizing on the benefits of metrics and ensuring the right information is being used and communicated effectively.

Examples of Metrics Discovered Through Literature Review		
emergency service response time	average time for change completion	loss amount per trip
persons who voluntarily showed identification badges versus those who did not	annual security costs in relation to annual revenue	password resets
security cost per employee	security incidents caused by improper access control configuration	adverse comments in customer surveys
network downtime	viruses detected in user files	alarm activations that run more than one minute before being turned off
security policy violations	percentage of information systems tested annually	systems that police will no longer respond to because of false alarms
percentage of user IDs belonging to people who have left the organization	viruses/trojans received	defective pieces of detection and signaling equipment
rate of employee turnover	weak password breaches reported by employees	discrepancies per delivery
percentage of employees whose background checks yield negative findings	hours spent on security-related issues	value of losses through discrepant deliveries
average time needed to conduct background checks	network downtime	percentage of searches that discover contraband
patients searched by emergency services at a hospital	countermeasures tested	value of property recovered
armed robberies at a specific store location	countermeasures deployed	inventory shrinkage
door alarm annunciations	incident response time	
cost or loss avoidance		

III. Metrics Communication

Regardless of the type of metric being used, communicating metric value remains a challenge. It does not matter how great the data is if it cannot be understood by key stakeholders (Dix, 2013). Corporate management tends to view security as overhead (i.e., a cost center rather than a production center) and security metrics as merely measuring activity, not value. Security professionals note that security benefits are difficult to measure compared to the benefits of profit centers, and such professionals often lack the skills or time to create and administer effective metrics. Thus, current security metrics, in practice, are generally not compelling and are often not taken seriously (Rothke, 2009). The literature does offer suggestions in terms of improving metric communication, including making metrics meaningful to key stakeholders, benchmarking, and demonstrating return on investment.

Metrics Communication Outline:

A. Making Metrics Meaningful to Key Stakeholders

    1. Tailor to Audience

    2. Communicate Based on Risk

    3. Measure and Communicate Over Time

B. Benchmarking

C. Return on Investment

D. Communicating Metrics – Concluding Remarks

A. Making Metrics Meaningful to Key Stakeholders

Prior to choosing a metric, security professionals should identify the data that is most important to executive management and other stakeholders; metrics should be selected and communicated in accordance with the data that is of most importance to the audience (Pironti, 2007). It is important to identify concrete objectives and goals in accordance with this information (McCourt, 2011). Based on this determination, it may be of most importance to assess programs, behavioral change, people performance, financials, evolutions in risk, etc. (Campbell, 2007). This forethought will greatly ease the process of communicating metric results and value to management. Additional techniques include tailoring the communication to the audience, communicating based on risk, and measuring and communicating over time.

1. Tailor to Audience

When communicating metrics, it is essential for the audience to include both executive management and technical specialists who are knowledgeable about the metric and its security content domain (Whitman & Mattord, 2012). Security professionals should define their metric values in terms that management will understand (Ting & Comings, 2010). One can be more persuasive by using metrics to tell a story—that is, by collecting metrics that are forward-looking and backward-looking and by addressing the questions "Where are we going?" and "Where have we been?" (Campbell, 2011; Blades, 2012). Security professionals can best explain their findings by providing specific, concrete examples that are meaningful to the audience (Deming, 2012).

To link security to the business, one source recommends that a metric should:

> "Be linked to an organization's missions and goals; be clearly stated; have quantifiable targets or other measurable values; be reasonably free of significant bias or manipulation that would distort the accurate assessment of performance; provide a reliable way to assess progress; sufficiently cover a program's core activities; have limited overlap with other measures; have balance, or not emphasize one or two priorities at the expense of others; [and] address enterprise-wide priorities" (ASIS & Institute of Finance & Management, 2013).

2. Communicate Based on Risk

In addition, metrics should be communicated in terms of the risks they are designed to mitigate. It is advantageous to discuss metrics and risks in terms of the probability of future events and the severity of the consequences if these events occur (Doinea & Pavel, 2010; Azuwa, Ahmad, Sahib, & Shamsuddin, 2012). Communicating statistics to executives can be challenging. When discussing and presenting risk-based data, it is important to also disclose the inherent uncertainties of the metrics used. Managers factor uncertainties into their daily decision-making; not communicating uncertainties leads to perceptions of dishonesty (Refining risk management, 2011). Security professionals are also advised to talk specifically about risks in terms of the actual business resources threatened and the value of these resources (Brenner, 2010). In "Leveraging Corporate Security for Business Growth and Improved Performance: The Transformative Effect of 9/11" (2012), the Conference Board Council of Corporate Security Executives names security metrics as part of building a security-aware culture. (The report is based on meetings that included the International Security Management Association and the CSO Roundtable of ASIS International.) The report notes, "It is up to an organization's top leadership, including the CSO, to change any lingering perceptions

that security is an imposition rather than an essential component of how you do business. Business units ultimately own the risk, with security as a critical partner, identifying those risks and developing ways to manage them."

3. Measure and Communicate Over Time

Lastly, it is essential to measure and communicate metric results over time. Ultimately, metrics are the marketing tool for the security program (McIIravey & Ohlhausen, 2012). Examining metric trends over time allows for meaningful comparisons to be made and can be a useful vehicle for communicating metric value and results. Metrics should be communicated in terms of the strategic goal they are linked to; progression toward this goal should be measured over time (Drugescu & Etges, 2006; Enescu, Enescu, & Sperdea, 2011). Incident management software (IMS) can help make organizing and discerning meaning from data (i.e., trends analysis) faster and less burdensome on personnel, and thus could serve as a crucial aid in efficient and effective communication (McIIravey & Ohlhausen, 2013).

B. Benchmarking

Benchmarking is a key tool used to help organizations communicate and qualify the state of their metrics. Benchmarking, simply put, involves comparing one's organization to another organization based on a pre-established and standardized measurement (GIA, 2010). Benchmarking data can be gathered by analysts, third-party consultants, individual employees, or publicly available surveys (Pironti, 2007). It is essential that benchmark selection be aligned with strategic organizational goals rather than solely based on appeasing management (Hayes & Kotwica, 2011). Products and services, processes, financial performance, and strategies can all be benchmarked. Benchmarking results in the establishment of best practices and learning across organizations. This technique grants organizations the opportunity to ascertain where they stand on a given metric in relation to their competitors. This results in a more effective interpretation of metric outcomes, and, in turn, more effective metric communication and a better-defined pathway toward improvement (GIA, 2010).

Unfortunately, the benchmarking approach is contingent on the availability of data, widespread use of the same metric, and organizations' willingness to share their data (McIIravey & Ohlhausen, 2012). Organizations and industry are often unwilling to share information (Wheeler, 2008). However, with the advent of social media, including Facebook, LinkedIn, and Twitter, information sharing is becoming more and more common (GIA, 2010). When available, strategically selected benchmarks can be a crucial aid in communication.

C. Return on Investment

Return on investment (ROI) is a widely known construct that can be applied to ensure effective metric communication. ROI can be a vehicle for metrics to justify budgets and can help in examining financial inputs and outputs of various security activities; these factors are of utmost importance to management and key stakeholders (Martin, Bulkan, & Klempt, 2011; Hastings, 2013). Unfortunately, calculating ROI is not straightforward, particularly in the security realm (Thompson, 2010). However, when available, ROI data can be a great tool to harness management attention and action. ROI calculations and applications are discussed further in the metrics evaluation section below.

D. Communicating Metrics – Concluding Remarks

This section explored the suggestions presented in the security literature to improve metric communication. Ways of making metrics meaningful to key stakeholders were explored; these include tailoring metrics and metric communication to the audience, communicating based on risk, and collecting and communicating data over time. Benchmarking is an additional communication aid, allowing organizations to see where they stand on a given metric in relation to their competitors; unfortunately, this approach is contingent on the widespread use of identical metrics and organizations' willingness to share their data. Communicating metrics based on ROI is another tactic used to illustrate the importance of the data being collected; however, this calculation is not straightforward (this discussion continues in the following section). At a high level, these strategies can help security practitioners better understand how to effectively communicate their metric, metric results, and metric value. The evaluation techniques presented in the following section can also be used to frame metric communications.

IV. Metrics Evaluation

Effective metric communication is irrelevant if one is not using a statistically sound measure. The movement toward the use, perceived value, and communicability of security metrics has also led to an increased interest in metric evaluation. Within the security realm, suggested evaluative factors include data automation (McIlravey & Ohlhausen, 2012), metric type (Campbell, 2007), relevance to organizational objectives (Prince, 2009), SMART criteria (Campbell, 2006), and return on investment (Martin, Bulkan, & Klempt, 2011). Outside the security realm, evaluative factors such as fairness, bias, reliability, and validity are emphasized within the context of personnel selection and educational and psychological testing (SIOP, 2003; AERA, APA, & NCME, 1999).

> Metrics Evaluation Outline:
> A. Current Practices in Security Metric Evaluation
> > 1. Data Automation
> > 2. Metric Type
> > 3. Relevance to Organizational Objectives
> > 4. SMART Criteria
> > 5. Return on Investment
> B. Metrics Evaluation – Beyond the Security Realm
> > 1. Reliability and Validity in Evaluation
> C. Security Metrics Evaluation – Concluding Remarks

A. Current Practices in Security Metric Evaluation

What makes a good metric? At present the security research focuses more on overarching themes, frameworks, and principles rather than specific, defined metric evaluation criteria. For example, hypothesis testing is one framework that can be used to assess metric value. This involves developing an overall hypothesis, related sub-hypotheses, and pertinent diagnostic questions that can be supported or disproved based on the metric and security domain of interest (Jaquith, 2007). Principles of measurement that should be employed include reproducibility, relevance, and timeliness (Jansen, 2009).

1. Data Automation

In addition to frameworks and principles, the ease and automation of data is a factor that can help determine metric effectiveness (Azuwa, Ahmad, Sahib, & Shamsuddin, 2012). Incident management software (IMS), for example, can deliver timely, orderly, and accurate security data in a variety of contexts (McIIravey & Ohlhausen, 2012; Dallas county uses DHS grant to grab incident management software, 2008). IBM offers Smarter Analytics software that allows organizations to combine consumer data with their internal data to identify patterns (Neeley, 2013). Cloud computing is an additional technology that can meaningfully automate data mining. For example, Data Tactics Corporation in Alexandria won a $24.8 million data mining contract with the Army to conduct cloud computing; in this case, cloud computing involves conducting data, event, and object extraction and mining on financial data, signals intelligence, video, audio, etc. (Keller, 2010). Automated information-sharing systems can also be assessed in terms of fiber-optic connections, network architecture, and geospatial information systems (Anderson, n.d.). However, automation does not guarantee infallible metrics. For example, data mining systems have been used to support counterterrorism; a report conducted by the Government Accountability Office highlights the challenges the Department of Homeland Security faces in ensuring the effectiveness of its system and privacy protections (GAO, 2011). Nonetheless, metrics that automatically yield reliable, accurate data are advantageous.

2. Metric Type

Metric type can be an additional categorization of existing metrics that can help foster effective metric evaluation. For example, a distinction can be made between descriptive and prescriptive metrics. Descriptive metrics focus on past performance, whereas prescriptive metrics focus on forecasting future performance. Prescriptive metrics have inherent advantages over descriptive metrics, including granting organizations a higher competitive edge and more advanced intelligence (McIIravey & Ohlhausen, 2012). The distinction between leading, lagging, and coincident indicators is another crucial distinction among metrics (see adjacent box; Campbell, 2007; Jansen, 2009).

> "A coincident indicator reflects security conditions happening concurrently, while leading and lagging indicators reflect security conditions that exist respectively before or after a shift in security" (Jansen, 2009, p. 6).

Another useful categorization of metrics is the contextual focus of the metric. For example, does the metric focus on cost or risk management? Is it based on a legal or policy requirement (Campbell, 2007)? An evaluation based on metric type would allow security professionals to best identify the metric that is most appropriate given the context of their organization.

3. Relevance to Organizational Objectives

Metrics should be also evaluated in terms of their relevance to high-level organizational objectives (Prince, 2009). Metrics should be tailored to address a specific business need (Rathbun, 2009). Although organizations are unique, organizations with similar work functions will share common objectives. Identifying what metrics are useful for a given purpose will help organizations choose metrics that are better-suited for their needs and make these choices faster. This identification would allow for metrics progression across organizations (Jansen, 2009).

4. SMART Criteria

SMART criteria can also be used to assess metric value. In order for metrics to be effective, they must be specific, measurable, attainable, relevant, and timely. These criteria will help ensure that metrics are quantifiable and that the user has measurable means of communicating risk to the organization's stakeholders (Campbell, 2006; Campbell, 2007; Martin, Bulkan, & Klempt, 2011; Payne, 2006).

5. Return on Investment

A return on investment (ROI) calculation examines gains or benefits attained per dollar spent. ROI can be applied to determine the effectiveness of a metric. A common objective for metrics is to justify budgets and to examine inputs and outputs (Martin, Bulkan, & Klempt, 2011; Hastings, 2013). Gathering impact and financial loss data is essential in order to make decisions related to information security (Baker, Rees, & Tippett, 2007). Unfortunately, ROI is not a straightforward measurement, particularly in the field of security.

> "Outside of compliance, it is becoming common for companies to actually reduce their security budgets because the nature of security can make it difficult to measure its worth" (Thompson, 2010, p.6).

However, the field of security is starting to advance in terms of a more defined operationalization of ROI. ROI should focus on both quantitative factors, such as dollar amounts, and qualitative factors, such as anticipated operational efficiency improvement and loss prevention (McLean & Brown, 2003; Harowitz, 2006). Pacl (2003) states that security ROI should focus on three factors: regulation, revenue, and reputation. Regulation refers to being in compliance with relevant laws, such as the Health Insurance Portability and Accountability Act. Revenue references profit in terms of a dollar amount. Reputation refers to the reactions and beliefs that key stakeholders would form and share with others should a breach in security occur (Pacl, 2003). This illustrates how metrics can demonstrate ROI, and the extent to which a metric can demonstrate ROI is a crucial determinant of the metric's effectiveness.

B. Metrics Evaluation – Beyond the Security Realm

Outside the security realm, behavioral scientists with a background in statistical analysis research have developed and employed various standards for evaluating metrics used in other fields, such as employee selection (SIOP, 2003) and educational measurement (e.g., AERA, APA, & NCME, 1999). The *Principles for the Validation and Use of Personnel Selection Procedures* (2003) and *Uniform Guidelines on Employee Selection Procedures* (1978) focus on fairness, bias, and adverse impact determinations. Subgroup differences are the degrees of difference between racial and gender subgroup scores typically observed for the instrument. This is relevant if the instrument is used in a way that will impact employee selection decisions (hiring, promotion, bonuses, certification, identification of employees for additional training, etc.). The *Standards for Educational and Psychological Testing* (1999) also examine fairness in testing.

In addition, Schmidt and Hunter (1998) examined personnel selection methods for variability and selection ratio (i.e., the number of applicants that are hired divided by the number of total

applicants). These measurement standards are crucial in determining the effectiveness of a metric. It is essential for security practitioners to also examine issues of fairness, bias, and variance. These factors are crucial in determining the validity and reliability of metrics, the importance of which is discussed in the following section.

1. Reliability and Validity in Evaluation

The *Uniform Guidelines on Employee Selection Procedures* (1978) and *Principles for the Validation and Use of Personnel Selection Procedures* (2003) were enacted to ensure the standardization of guidelines used to evaluate employee selection procedures in accordance with federal law. The *Standards for Educational and Psychological Testing* (1999) provides standards against which to evaluate educational and psychological measurements. Each document provides stringent guidelines in terms of effectively demonstrating evidence for reliability and validity.

Reliability is the degree to which the metric yields reliable scores as measured by traditional psychometric methods such as test-retest, internal consistency, or parallel forms reliability. Validity refers to the degree of cumulative evidence in the research literature, or original studies conducted by the user, supporting inferences drawn from the metric. The *Uniform Guidelines on Employee Selection Procedures* (1978) provides guidelines surrounding three types of validity (content, criterion, and construct) and their corresponding technical standards. The *Principles for the Validation and Use of Personnel Selection Procedures* (2003) and the *Standards for Educational and Psychological Testing* (1999) also provide guidance on the sufficiency and types of validity and reliability evidence that should be collected.

Consequential validity is an additional component of validity that should be considered when evaluating metrics; it means the extent to which use of the metric is free from unintended negative consequences, such as an undue time burden on staff. Although not mentioned explicitly in the security literature, this concept is illustrated through the following quotes:

> "Such is the pressure in some organisations to meet targets that some may be led to engage in fiddling or lesser tactics to meet the metric. Such approaches might include the non-reporting of events, discouragement of reporting by third parties, reassigning incidents and completely fabricating data" (Aleem, Wakefield, & Button, 2013, p.246).
>
> "The harder [a metric is] to collect and the longer it takes people to collect it the less likely it is to succeed over time, because people are just going to get frustrated with it" Jones, Kodak (Prince, 2009, para. 11).

Validity can also be illustrated through the generalizability of the measure to other situations, samples, tests, etc. (Straub, Hoffman, Weber, & Steinfield, 2002). Concepts similar to validity include the notions of correctness and effectiveness as described by Jansen (2006).

C. Security Metrics Evaluation – Concluding Remarks

The security literature discusses many factors that should be examined when determining the effectiveness of a metric, including ROI, metric type, data automation, SMART criteria, relevance to organizational objectives, etc. However, it is important to note that these factors are generally presented only at a conceptual level within the security literature. Definitions that yield specific

measurements are not provided; the evidence needed to show that these factors are met is not discussed; examples of metrics that illustrate the desired measurement criteria are not provided.

In addition, explicit empirical evidence regarding security metric validity and reliability information is absent from the security literature; this is a crucial gap that must be addressed. If a metric is not reliable or valid, then the conclusions drawn from it will be inaccurate. For example, if the number of door alarm annunciations increases tenfold in one month, a security professional might conclude that this represents an increase in attempted burglaries; however, this increase could merely be due to a faulty door alarm system. Drawing inaccurate conclusions and communicating misinformation would undermine the security professional's attempt at describing and improving security, which in turn would drive management to further underestimate the importance of security and security metrics.

Overall Conclusions:

- Descriptions of existing security metrics are often vague, making it difficult to adopt those metrics. The focus is more on counting events than creating meaningful, risk-based metrics.

- Strategies for communicating metrics are general and may be hard to implement.

- Typically, evaluation criteria are only presented at a conceptual level within the security literature, without explicit definitions.

- Few examples of empirically sound metrics (with statistical justification and evidence) are present within the security literature. Physical security and information security appear to have more metrics in use than other security fields.

- The development of the Security Metrics Evaluation Tool (Security MET) will address these limitations.

V. Conclusion

Without compelling metrics, security professionals, and the budgets that power their operations, continue largely on the intuition of company leadership. With metrics, the security function grounds itself on measurable results that correlate with investment, and the security professional can speak to leadership in a familiar business language. The purpose of this review was to synthesize literature surrounding existing metrics, communicating metrics, and evaluating metrics. This work will help security professionals better comprehend metrics that are currently in use, more effectively present metrics to executive management in a persuasive manner, and more comprehensively evaluate existing metrics.

The present literature review identified a gap regarding the existence and evaluation of statistically sound metrics. Existing metrics are generally presented only at a conceptual level; it is difficult to ascertain what specifically is being measured, how this measurement is obtained, and when the measurement should be used. As such, duplicating the measures presented would likely not be a straightforward process. In addition, the present focus of security metrics remains more on summative indicators rather than meaningful, risk-based metrics (Hayes & Kotwica, 2012). Also, the communication strategies proposed within the security literature, including tailoring metrics to the audience, return on investment, and benchmarking, are general guidelines; the implementation of these guidelines would likely not be straightforward. In addition, the evaluative factors presented within the security literature (including metric type, relevance to organizational objectives, etc.) are only provided at a conceptual level. Reliability and validity are also not meaningfully explored within the security literature. Examples of metrics that illustrate the desired evaluation criteria, and measurable definitions of these criteria, were not found in the security literature. Physical security and information security appear to have more metrics in use than other security fields.

The development of the Security Metrics Evaluation Tool (Security MET) will address these gaps. The Security MET will provide a framework and explicit statistical and business criteria that will advance the field of security metrics by providing a vehicle through which metrics can be grounded in risk assessment, key business goals and objectives, and the principles of measurement; this process, in turn, will help ensure the effective communication of metrics by providing specific criteria to discuss. The Security MET will be sufficiently robust so that it can be applied to develop metrics across the various security domains, business functions, etc.

Security metrics allow organizations to hold individuals accountable for specified results and goals, and they are a vehicle through which security programs can demonstrate their measurable impact on an organization's strategic, organizational, financial, and operational risks and profits (Campbell, 2007). Therefore, it is paramount to advance the understanding of which metrics are in use, how to effectively communicate metrics, and what makes a good metric.

VI. References

Aleem, A., Wakefield, A., & Button, M. (2013). Addressing the weakest link: Implementing converged security. *Security Journal, 26*, 236-248.

American Educational Research Association (AERA), American Psychological Association (APA), & National Council on Measurement in Education (NCME). (1999). *Standards for educational and psychological testing*. Washington, D.C.

Anderson, T. (2004). From small clues to big picture. *Security Management*. Retrieved from http://www.securitymanagement.com/article/small-clues-big-picture.

ASIS International and Institute of Finance & Management. (2013). *The United States security industry: Size and scope, insights, trends, and data*. Alexandria, VA: ASIS International.

Azuwa, M., Ahmad, R., Sahib, S., & Shamsuddin, S. (2012). Technical security metrics model in compliance with ISO/IEC 27001 standard. *International Journal of Cyber-Security and Digital Forensics, 1*(4), 280-288.

Baker, W., Rees, L., & Tippett, P. (2007). Necessary measures: Metric-driven information security risk assessment and decision making. *Communications of the ACM, 50*(10), 101-106.

Berinato, S. (2005). A few good information security metrics. *CSO Online*. Retrieved from http://www.csoonline.com/article/220462/a-few-good-information-security-metrics.

Bewley, S. (2013). Lack of big data means big problems for pay tv. *Multichannel News*.

Blades, M. (2012). Delivering meaningful metrics. *Security Magazine*. Retrieved from http://www.securitymagazine.com/articles/82934-delivering-meaningful-metrics.

Brenner, B. (2010). Security metric techniques: How to answer the 'so what?' *CSO Online*. Retrieved from http://www.csoonline.com/article/602901/security-metric-techniques-how-to-answer-the-so-what-.

Burns, F., Bystrov, A., Koelmans, A., & Yakolev, A. (2011). Design and security evaluation of balanced 1-of-n circuits. *IET Computers and Digital Techniques, 6*(2), 125-135.

Campbell, G. (2006). How to use metrics. *CSO Online*. Retrieved from http://www.csoonline.com/article/220980/how-to-use-metrics.

Campbell, G. (2007). *Measures and metrics in corporate security: Communicating business value*. Framingham, MA: CSO Executive Council.

Campbell, G. (2011). Metrics for success. *Securityinfowatch*. Retrieved from http://www.securityinfowatch.com/article/10517904/metrics-for-success.

Campbell, G. (2012). Metrics for success: Security operations control center metrics. *Securityinfowatch*. Retrieved from http://www.securityinfowatch.com/article/10840065/metrics-for-success-security-operations-control-center-metrics.

Carnegie Mellon University. (1995). Security metrics. In *systems security engineering-capability maturity model*. Retrieved from http://web.archive.org/web/20120423172421/http:/www.sse-cmm.org/metric/metric.asp.

Case study: Hershey Entertainment & Resorts. (n.d.). *iVIEWSYSTEMS*. Retrieved from http://www. iviewsystems.com/case-study---hershey-entertainment---resorts.

Casola, V., Mazzeo, A., Mazzocca, N., & Vittorini, V. (2007). A policy-based methodology for security evaluation: A security metric for public key infrastructures. *Journal of Computer Security, 15,* 197-229.

Chew, E., Clay, A., Hash, J., Bartol, N., & Brown, A. (2006). Guide for Developing Performance Metrics for Information Security. *NIST Special Publication 800-80 Revision 1*. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-55-Rev1/SP800-55-rev1.pdf.

Cisco 2010 annual security report: Highlighting global security threats and trends. (2010). Retrieved from http://www.cisco.com/go/securityreport.

CIS consensus information security metrics (n.d.). *Security Benchmarks*. Retrieved from http:// benchmarks.cisecurity.org/downloads/metrics.

Collins, B. (2004). Information security program metrics. In *Security Business Practices Reference 6,* 20-21. Alexandria, VA: ASIS International.

Conference Board Council of Corporate Security Executives. (2012). Leveraging corporate security for business growth and improved performance: The transformative effect of 9/11. Retrieved from http://www.ssr-personnel.com/CSO_RT_ISMA_TCB_Paper.pdf.

Dallas county uses DHS grant to grab incident management software (2008). *Security Magazine*. Retrieved from http://www.securitymagazine.com/articles/dallas-county-uses-dhs-grant-to-grab-incident-management-software-1.

Davenport, T. (2009). Make better decisions. *Harvard Business Review*. Retrieved from http://hbr. org/2009/11/make-better-decisions/ar/1.

Davenport, T., & Harris, J. (2010). Analytics and the bottom line: How organizations build success. Key Learning Summary published by *Harvard Business Review*.

Deming, P. (2012). Proving security's value: Demonstrating the value of security in terms of cost savings can make a difference when budget dollars are allocated. *Security Management*. Retrieved from https://cso.asisonline.org/KnowledgeCenter/Library/2012/ Documents/0912ProvingSecurity'sValue_Managing.pdf

Dix, J. (2013). Big data the security answer? *NETWORKWORLD*. Retrieved from http://www. networkworld.com/columnists/2013/031113-edit.html.

Doinea, M., & Pavel, S. (2010). Security optimization for distributed applications oriented on very large data sets. *Informatica Economică, 14*(2), 72-85.

Drugescu, C., & Etges, R. (2006). Maximizing the return on investment of information security programs: program governance and metrics. *Information System Security*, 30-40.

Embracing big data can lead to greater security (2013). *COMPUTERWEEKLY.*

Enescu, M., Enescu, M., & Sperdea, N. (2011). The specifics of security management: The functions of information security required by organizations. *Economics, Management, and Financial Markets 6*(2), 200-205.

Garcia, M. L. (2006). *Vulnerability assessment of physical protection systems.* Boston, MA: Butterworth-Heinemann.

Garcia, M. L. (2008). *The design and evaluation of physical protection systems* (2d ed). Boston, MA: Butterworth-Heinemann.

Garigue, R., & Stefaniu, M. (2003). Information security governance reporting. *Security Management,* 36-40.

Gauging security ROI (2007). *Journal of Accountancy,* 19.

Getting started using performance metrics (2005). *Security Director's Report, 5*(4), 11-12.

GIA (2010). *How social media is redefining benchmarking* [White Paper]. Retrieved from http://www.globalintelligence.com/press/latest/2010/gia-white-paper-explains-how-social-media-are-redefining-competitive-benchmarking.

Gips, M. (2004). Powering up log auditing. *Security Management.* Retrieved from http://www.securitymanagement.com/article/powering-log-auditing.

Gill, M., Burns-Howell, T., Keats, G. & Taylor, E. (2007). Demonstrating the value of security. Leicester, UK: Perpetuity Research & Consultancy International.

Government Accountability Office. (2011). *Data mining: DHS needs to improve executive oversight of systems supporting counterterrorism.* Retrieved 2013, June 10 from http://www.gao.gov/new.items/d11742.pdf.

Guidelines and Metrics Working Group, ASIS Defense and Intelligence Council (2012). "Watch us build an effective security performance metric that will work for you and your boss, then build your own, or influencing effective corporate management behavior through compelling performance metrics," presentation at the ASIS International 58th Annual Seminar and Exhibits, Philadelphia.

Harowitz, S. (2006). Challenges and trends. *Security Management.* Retrieved from http://www.securitymanagement.com/article/challenges-and-trends.

Hastings, R. (2013). *Achieving sector resilience through enhancing physical protection: An analysis of the Canadian banking sector* (Masters Thesis). Carleton University, Ottawa, Ontario.

Hayes, B., & Kotwica, K. (2012). Advances and stalemates in security. *Security Magazine,* 34.

Hayes, B., & Kotwica, K. (2011). Benchmarks aren't magic, they're tools. *Security Magazine.* Retrieved from http://www.securitymagazine.com/articles/82320-benchmarks-arent-magic-theyre-tools.

Health Resource Network, Inc. (2000). *ASIS healthcare security committee healthcare security benchmarking study.* Florham Park, New Jersey.

How metrics can link security to the business (2011). *Security Director's Report, 11*(4), 10-12.

Huff, A. (2013). Big data I: Exception monitoring. *Commercial Carrier Journal.* Retrieved from http://www.highbeam.com/doc/1G1-324762775.html.

Interagency Security Committee. (2013). *The risk management process for federal facilities: An Interagency Security Committee standard*. Retrieved from http://www.dhs.gov/sites/default/files/publications/ISC_Risk-Management-Process_Aug_2013.pdf.

ISO/IEC. (2005a). Information technology — Security techniques — Information security management systems — Requirements. *ISO/IEC 27001*. Retrieved from http://www.iso27001security.com/html/27001.html.

ISO/IEC. (2005b). Information technology — Security techniques — Code of practice for information security management. *ISO/IEC 27002*. Retrieved from http://www.iso27001security.com/html/27002.html.

ISO27K (2007). *ISO/IEC 27001 & 27002 implementation guidance and metrics*. Prepared by the international community of ISO27k implementers at ISO27001security.com.

Jansen, W. (2009). Directions in Security Metrics Research. *NIST*. Retrieved 2013, June 10 from http://csrc.nist.gov/publications/nistir/ir7564/nistir-7564_metrics-research.pdf.

Jaquith, A. (2007). *Security metrics: Replacing fear, uncertainty, and doubt*. Upper Saddle River, NJ: Addison-Wesley.

Keller, J. (2010). Intelligence gathering in the cloud: Data tactics wins Army cloud computing data mining contract. *Military & Aerospace Electronics*.

Kiron, D., Shockley, R., Kruschwitz, N., Finch, G., & Haydock, M. (2011). Analytics: the widening divide; How companies are achieving competitive advantage through analytics. *IBM Global Business Services/MIT Sloan Management Review*. Retrieved from http://public.dhe.ibm.com/common/ssi/ecm/en/gbe03448usen/GBE03448USEN.PDF

Kovacich, G., & Halibozek, E. (2006). *Security Metrics Management*. Boston, MA: Butterworth-Heinemann.

Martin, C., Bulkan, A., & Klempt, P. (2011). Security excellence from a total quality management approach. *Total Quality Management, 22*(3), 345-371.

Mayor, T. (2006). Ideas you can steal from Six Sigma: Tips for improving the effectiveness and efficiency of physical and information security. *CSO Online*. Retrieved from http://www.csoonline.com/article/221094/ideas-you-can-steal-from-six-sigma.

McCourt, M. (2011). Measuring up: How the best security leaders deliver business value. *Security Magazine,* 16-27.

McLean, G. & Brown, J. (2003). Determining the ROI in IT security. *CAmagazine*. Retrieved from http://www.camagazine.com/archives/print-edition/2003/april/upfront/news-and-trends/camagazine23257.aspx.

McIIravey, B., & Ohlhausen, P. (2012). *Metrics and analysis in security management* [White Paper]. Retrieved from http://www.ppm2000.com/resources/white_papers.asp.

McIIravey, B., & Ohlhausen, P. (2013). *Strengthening intelligence and investigations with incident management software* [White Paper]. Retrieved from http://www.ppm2000.com/resources/white_papers.asp.

Neeley, P. (2013). From details to desires: the power of big data. *Marketing Week*, 11. Retrieved from http://connection.ebscohost.com/c/articles/88255689/from-details-desires-power-big-data.

Pacl, B. (2003). Security ROI: Know what to measure. *Communications News*, 18.

Payne, S. (2006). *A guide to security metrics* [White Paper]. Retrieved from http://www.sans.org/reading_room/whitepapers/auditing/guide-security-metrics_55.

Pironti, J. (2007). Developing metrics for effective information security governance. *ISACA, 2*. Retrieved from http://www.isaca.org/Journal/Past-Issues/2007/Volume-2/Pages/Developing-Metrics-for-Effective-Information-Security-Governance1.aspx.

Prince, B. (2009). Developing security metrics for enterprise risk management. *eWEEK*. Retrieved from http://www.eweek.com/c/a/Security/Developing-Security-Metrics-for-Enterprise-Risk-Management-745202.

Rathbun, D. (2009). *Gathering security metrics and reaping the rewards* [White Paper]. Retrieved from http://www.sans.org/reading_room/whitepapers/leadership/gathering-security-metrics-reaping-rewards_33234.

Ravenel, J. (2006). Effective operational security metrics. *Security Management,* 10-17.

Refining risk management (2011). *Security Management,* 20-21. Retrieved from https://cso.asisonline.org/KnowledgeCenter/Library/2011/Documents/1111RefiningRiskManagement_Intel.pdf.

Rothke, B. (2009). The security laugh metric. *Network World Asia,* 36.

Scaglione, B. (2012). Metrics: The evaluation of access control and identification. *Security Magazine.* Retrieved from http://www.securitymagazine.com/articles/83134-metrics--the-evaluation-of-access-control-and-identification.

Schmidt, F., & Hunter, J. (1998). The validity and utility of selection methods in personnel psychology: Practical and theoretical implications of 85 years of research findings. *Psychological Bulletin, 124*(2), 262-274.

Society for Industrial & Organizational Psychology (SIOP) (2003). *Principles for the validation and use of personnel selection procedures* (4th edition). Bowling Green, OH.

Sternstein, A. (2013). Taking a flier on big data. *Government Executive, 45*(3), 24-26.

Straub, D., Hoffman, D., Weber, B., and Steinfield, C. (2002). Toward new metrics for net-enhanced organizations. *Information Systems Research, 13*(3), 227-238.

Thompson, H. (2010). Practical security metrics: Effective security practices series. Retrieved 2013, June 10 from http://www.microsoft.com/en-us/download/details.aspx?id=1537

Ting, W. & Comings, D. (2010). Information assurance metric for assessing NIST's monitoring step in the risk management framework. *Information Security Journal: A Global Perspective, 19*, 253-262.

Treece, D. & Freadman, M. (2010). Metrics is not a four-letter word. *Security Magazine,* 90-94.

Uniform guidelines on employee selection procedures (1978). Retrieved 2013, June 10 from http://www.shrm.org/LegalIssues/FederalResources/FederalStatutesRegulationsandGuidanc/Pages/Uniformguidelinesonselectionprocedures.aspx.

Van Till, S. (2013). How will big data change security? *SecurityMagazine.* Retrieved from http://www.securitymagazine.com/articles/84179-how-will-big-data-change-security.

Vellani, K. (2004). Achieving return on investment from crime analysis. In *Security business practices reference*, 35-36. Alexandria, VA: ASIS International.

Wagley, J. (2007). Sizing up enterprise rights management. *Security Management.* Retrieved from http://www.securitymanagement.com/article/sizing-enterprise-rights-management.

Wailgum, T. (2005). Metrics for corporate and physical security programs. *CSO Online.* Retrieved from http://www.csoonline.com/article/220023/metrics-for-corporate-and-physical-security-programs.

Wheeler, T. (2008). Organization security metrics: Can organizations protect themselves? *Information Security Journal: A Global Perspective, 17,* 228-242.

Whitman, M. & Mattord, H. (2012). Information security governance for the non-security business executive

Appendix D: Online Survey

The research team invited more than 3,000 ASIS members to participate in an online survey. Invitations were sent to all ASIS council members and the CSO Roundtable, plus an ASIS-created pool of top-level security professionals.

Specifically, the ASIS IT Department pulled the names of all ASIS council members (775), all CSO Roundtable members (320), and all ASIS members with titles of "director" and above (4,521). The pool was selected as being more likely to include metrics users (compared to a random sample of ASIS members). After the list was deduplicated and corrected, a link to the survey was e-mailed to 3,304 individuals. Of the e-mails sent, 95 percent were successfully delivered. Of those, 22 percent were opened. Of those opened, 43 percent led to survey participation. A total of 297 people responded to the survey.

This data collection process was not designed to determine the prevalence of security metrics use in the security profession generally (e.g., to learn that 22 percent of security managers use security metrics). Instead, it was designed to uncover specific instances of security metrics use (for follow-up interviews) and gain an understanding of the different ways in which security professionals may be using metrics.

I. Invitation to Participate

E-mail subject line: Metrics in Security: Share Your Insights and Strengthen Your Profession

ASIS Survey

Strengthen Your Profession:

Help Build Security's Use of Metrics

Security metrics are quantifiable measurements of an aspect of a system or enterprise, collected and analyzed to help an organization protect its people, property, and information. Using various metrics, security can measure results that correlate with investment and speak to leadership in familiar business language. Currently the field lacks tested metrics as well as guidance on effectively communicating metrics to executive management.

Two groups within ASIS are studying security metrics. By participating in their short, shared online survey, you can support both projects at once.

- The ASIS Leadership and Management Practices Council (LMPC) is capturing a snapshot of how security practitioners use metrics today.

- The ASIS Foundation has funded the Security Metrics Research Project, which aims to develop a tool for evaluating current and future metrics. The project will produce (1) an evaluation tool that security professionals can self-administer to develop and improve security metrics; (2) a database of selected, evaluated security metrics; and (3) guidelines for effective use of security metrics to demonstrate return on investment.

You are part of a select group of security professionals whose insights are being solicited for these two important projects.

Please take a moment to complete this short, important survey. Estimated time: 10 minutes.

Thank you!

ASIS Leadership and Management Practices Council
ASIS Foundation Security Metrics Research Project
More information: Barbara.Buzzell@asisonline.org

II. Survey Results by Question

Survey results are presented by question. The total sample for the survey included 297 participants. Note that not all participants answered every question, and that participants could select multiple responses for some questions. Also note that open-ended responses with a sample size of greater than 35 participants were categorized to ease in results interpretation (with the exception of questions pertaining to participant contact information). Each response was coded in up to two categories to ensure that the coding was comprehensive. The questions are presented below:

Q1: Collection And Use Of Security Metrics

Q2: Metric Comparison To External Benchmarks

Q3: Would You Use Metrics?

Q4: Measured Security Program Aspects

Q5: Who Records Metrics?

Q6: Metrics Provisions To Non-Security Persons

Q7: Metrics Provisions To Non-Security Persons – If No, Why Not?

Q8: Metrics Provisions To Non-Security Persons – Who?

Q9: Metrics Provisions To Non-Security Persons – How Often?

Q10: Metric Elements Shared With C-Suite Personnel

Q11: Most Important Metrics – Senior Management

Q12: Most Important Metrics – Why?

Q13: Metric Alignment With Risk/Objectives

Q14: Metric Alignment With Risk/Objectives – How?

Q15: Dashboard Tool Usage

Q16: Who Developed Dashboard Tool?

Q17: Third-Party Dashboard Tool Name

Q18: Metrics Interview Volunteers

Q19: Work Region

Q20: Desire Information Regarding Metrics

Given the limitations of the sample (e.g., participation was optional, and those who chose to participate probably are not representative of all security managers), the survey was not meant to ascertain the prevalence of particular metrics practices in the field but instead to discover metrics practices and identify metrics users for follow-up interviews.

Q1: Collection and Use of Security Metrics

1. Are you collecting and using security metrics? (Security metrics are quantifiable measurements of an aspect of a system or enterprise, collected and analyzed to help an organization protect its people, property, and information.)

Answer Options	Response %	Response Count
Yes	76.5%	225
No	23.5%	69

1. Are you collecting and using security metrics?

(Security metrics are quantifiable measurements of an aspect of a
system or enterprise, collected and analyzed to help an
organization protect its people, property, and information.)

23.5%

76.5%

Yes
No

Q2: Metric Comparison to External Benchmarks

2. Do you compare your metrics to any external benchmarks?

Answer Options	Response %	Response Count
Yes	38.8%	85
No	61.2%	134
If yes, please name or describe those benchmarks.		60

1) For security officer suppliers, industry benchmarks on turnover and training.

2) We look at other retailer's shortage metrics and investigative metrics (internal and external cases).

3) We benchmark often with like organizations (informal) and we assess our programs against benchmarks established by ISMA, OSAC, ASIS, PSIC, etc.

4) Compare against competitors in the marketplace as well as year over year performance

5) Local CAP reports and crime stats; discussions with similar properties and lines of business; industry publications and reports

6) DoD Benchmarks

7) Industry reports from big four and local companies

8) Depends on the metrics and the external counterpart

9) Other telecommunications operations and retail segments

10) ISMA, ASIS Benchmarks by the USC

11) Crime rates at other HOA's

12) We compare our metrics with other bank security directors and with American Banking Association (banking industry group) statistics.

13) Other peer organizations and through industry trade group (ABA)

14) ASIS and ISMA benchmark surveys.

15) Currently No, but will do so in near future

16) Police data

17) ASIS, Local and Federal Law Enforcement summaries, State Department information

18) Telecom Industry primarily

19) Not really. Unfortunately, comparable data across the security industry really isn't there. There really isn't much way either because the data would likely be very different from sector to sector.

20) Numbers, losses, recoveries, adverted losses of reported cases of internal (non claims) fraud within the company (insurance business) on a global scale.

21)	ASIS/ANSI/ISO Standards, Core Business practices based in TQM.
22)	SC-ISAC Cargo Theft Report CargoNet Cargo Theft reports
23)	Organizations with similar constituencies, size, geographic demographics
24)	Operational KPI's; financial benchmarks; facilities and geolocation; staffing levels & allocations; SLA's
25)	The eBenchmarks are set based on data collected from sister hospitals as well as surrounding similar hospitals
26)	Various crisis management benchmarks ISMA and ASIS benchmarks BOMA and other facility benchmarks as it relates to operational security costs per square foot
27)	United Nations Dept. of Safety and Security Threat and Risk Matrix.
28)	External response times; save rates; investigative costs; Liability costs; clearance processing times; system approval times
29)	In select areas where we have comparable/like data points for functions. For example span of control, ratios of staff per associate, security cost per associate etc.
30)	Cost of security as a % or revenue. Cost of security CAPEX. Number of security employees to workforce.
31)	Compare to peer companies
32)	We have a standard checklist across the board with standards
33)	Benchmark for academic medical centers in the Netherlands.
34)	Police metrics
35)	Figures reflecting the typical expenditure on physical security from IFMA and BOMA
36)	Neighboring crime statistics
37)	Gartner
38)	We benchmark all operations and technology every two years. It is usually a formal survey form which we apply in person when interviewing fellow security professionals
39)	All company plants worldwide
40)	Best Practices in similar industry
41)	# Job related kidnap incidents, #travel related security incident, #operations disruptions from a. Community b. labor activities etc.
42)	Call Center Metrics
43)	Theft, comparing number of events and amounts versus other companies
44)	Financial and industry standard benchmarks.
45)	National crime statistics. Other security metrics to corporations with similar situations, market, organization.

46)	Use various industry benchmarks. Some examples are Corporate Governance and Compliance Hotline Benchmarking Report, Krolls Global Fraud report.
47)	When possible, we compare average wage paid to security officers to the state labor statistics. Incident rates are compared to local crime rates.
48)	1. Vendor information 2. Academic peer review journals 3. Internal data 4. Benchmarking of like companies
49)	But have looked at doing so. Other companies with similar missions.
50)	Numbers related to reportable incidents
51)	FBI bank crime stats Ad hoc benchmarking for other security and fraud stats
52)	ASIS published data, Security 500, independent surveys, CSO Roundtable surveys, ISMA surveys.
53)	Similar companies
54)	With Pharmaceutical industry
55)	ASIS standards Other peers Regulatory standards
56)	Access control measures, investigative numbers on demographics,
57)	Compare supply chain losses, number of incidents and dollar amount to industry average.
58)	Organizational goals
59)	I have been unable to identify pertinent benchmark data that would allow for comparison.
60)	ISO27001

Qualitative Results: 2. Do you compare your metrics to any external benchmarks?

If yes, please name or describe those benchmarks.

Category Type:	Category:	Assigned Category #1		Assigned Category #2*	
		Response Count	Response %	Response Count	Response %
Benchmarking Source:	Established Benchmarks/ Standards	17	28.3%	7	11.7%
	Similar Organizations	15	25.0%	4	6.7%
	Industry/Agency Reports	4	6.7%	1	1.7%
	Industry/Agency Surveys	1	1.7%	2	3.3%
Benchmarking Type:	Security/Safety	10	16.7%	1	1.7%
	Operations	2	3.3%	1	1.7%
	Finance	2	3.3%	7	11.7%
	Performance	1	1.7%	1	1.7%
Other:	Other	8	13.3%	0	0.0%

*Note that some responses pertained to multiple categories and thus had 2 assigned categories.

2. Do you compare your metrics to any external benchmarks?

38.8%

61.2%

Yes
No

Q3: Would You Use Metrics?

3. If "No", would you use metrics if you knew more about how to create them and use them effectively?

Answer Options	Response %	Response Count
Yes	77.9%	53
No	22.1%	15

3. If "No", would you use metrics if you knew more about how to create them and use them effectively?

EFFECTIVE, EVALUATED SECURITY METRICS—© ASIS Foundation 2014

Q4: Measured Security Program Aspects

4. What aspects of the security program are measured to determine current performance levels/ program effectiveness? (Check all that apply)

Answer Options	Response %	Response Count
Guarding performance (turnover, inspections, etc.)	61.1%	127
Cost against budget	65.9%	137
Criminal incidents and investigations	69.2%	144
Security incidents	90.9%	189
Security training and education	62.5%	130
Communication and awareness programs	39.4%	82
Systems performance/downtime (CCTV/ Access Control/ Alarm systems)	40.4%	84
Regulatory compliance	43.3%	90
Physical security	60.6%	126
Background screening	30.3%	63
Risk analysis process	39.4%	82
Audit implications	30.8%	64
Internal customer satisfaction	37.0%	77
Other (Please specify what other aspects of security you are measuring.)		20

1) Safety Incidents

2) Call response & Closure
   Service response & Closure
   Alarm/Event Response & Closure
   Operator effectiveness

3) We also own the Ergonomics program so we compare HR claims and $$ to ergo consultations over time.

4) Service requests for all types of protective services, investigative and consultative needs

5) Losses

6) Safety

7) Program consistency with organizational goals

8) Physical Security System Exception Data

9) Follow the DOE process using design basis threat statements to determine security system goals and then use performance tests and tabletops to validate performance and drive corrective action.

10)	Emergency medical incidents, law enforcement incidents
11)	Return on Security Investment
12)	Personnel / executive protection, emergency response preparedness,
13)	International Travel Statistics
14)	Revenue protection Business impact analysis. Crisis Management ability.
15)	External Fraud
16)	GPS tracking by location of officer's ON POST or security patrols conducted.
17)	Visitor and access management numbers
18)	Costs as a percent of revenue, Security costs (as a percentage) relative to other functions, i.e., HR, EHS, Finance, etc.; measuring proactive time (assessing & managing risks) vs. reactive (investigation, responding to problems); setting and measuring performance against established targets, such as security awareness training, etc.
19)	Status of projects (electronic system installations), cost recoveries and reductions.
20)	RESPONSE TIME TO INCIDENTS

Q5: Who Records Metrics?

5. Typically, who is responsible for recording these metrics?

Answer Options	Response %	Response Count
Third party provider	14.0%	29
Internal Security Department Manager/Specialist	77.8%	161
System/Department Administrator	12.1%	25
Individual responsible for the element being measured	28.0%	58
Other (please specify)		9

1) Collected by individual responsible, collated by Security Department Manager

2) Each functional area reports monthly metrics and one admin compiles the reports.

3) Could be all of the above depending on the topic

4) Our 24x7 Security Support Center

5) Myself for metrics the client wants to keep track of.

6) Internal audit, HR, TQM.

7) Security Manager

8) Myself - security consultant

9) The manager responsible for the metrics provides Info/data. Assisted by department administrator.

5. Typically, who is responsible for recording these metrics?

Q6: Metrics Provisions to Non-Security Persons

6. Does security provide these metrics to persons outside the department?

Answer Options	Response %	ResponseCount
Yes	80.4%	168
No	19.6%	41

6. Does security provide these metrics to persons outside the department?

80.4%

19.6%

Yes
No

Q7: Metrics Provisions To Non-Security Persons – If No, Why Not?

7. If "No", why not?

Responses	28
1) Internal policy	
2) We track internal metrics to the client's security management	
3) Used to assess maintenance process within department.	
4) Prevent vulnerabilities	
5) Private	
6) Privacy	
7) For our eyes only and risk of "wrong conclusions"	
8) Confidentiality information	
9) Our general counsel believes this information is proprietary and should not be disclosed outside the legal/security group.	
10) Information is used to measure and improve internal process. The information would only be provided upon request to outside departments. Executive level security management (CSO) may provide information to CFO and CEO routinely, but I cannot confirm that is the case.	
11) Kept internally and have never been asked to share or provide support for global security program	
12) Internally initiated.	
13) It is an internal system on SharePoint	
14) Government entity. Likely to hide poor performance.	
15) Not as complete as I would like to be able to share.	
16) Other departments have not been interested or have not advised of a need for the information	
17) Company policy	
18) They are very specific to the guard force only.	
19) Legislation oblige to keep it confidential	
20) Having difficulty developing metrics that are of value to business leaders.	
21) Not real net to other business entities except business controls.	
22) Proprietary data is mixed in with external data and marked confidential	
23) All theses records are used in order to increase the security level but not to communicate	
24) Internal purpose only	

25) It is for internal purposes only.
26) No interest by other departments.
27) Airing laundry…
28) Governmental controls.

Q8: Metrics Provisions To Non-Security Persons – Who?

8. If Security provides these metrics to persons outside the department, to whom are the metrics provided? (Select all that apply.)

Answer Options	Response%	Response Count
Persons who report to you (your direct reports)	47.3%	78
Supervisor and/or supervisory chain	50.9%	84
Managers of other departments (Human Resources, Legal, Operations, etc.)	59.4%	98
Members of senior management (such as chief executive officer, chief information officer, chief financial officer, etc.)	79.4%	131
Other (please specify)		22

1) Customer representative

2) State Dept. of Education and Federal OCJP

3) N/A

4) Other security departments

5) Executive Committee (CEO, COO, CFO, CIO, CLO, etc.)

6) If requested by third parties

7) Board members also receive metrics reports in accordance with a federal law - the Bank Protection Act.

8) Not providing to outside party

9) External Customers (Clients)

10) Customers and subscribers

11) Risk & Compliance Committee

12) Protocol Service

13) Contract management firms

14) It all depends on the customer and the measurement.

15) Security Council

16) The survey becomes part of our annual report

17) Environment of Care Committee

18) Regulator, police, the board.

19) NA

20) Self-security consultant

21) Provided through roll-up report with other safety & physical environment metrics

22) CUSTOMERS

If Security provides these metrics to persons outside the department, to whom are the metrics provided? (Select all that apply.)

Category	Percentage
Persons who report to you (your direct reports)	47.3%
Supervisor and/or supervisory chain	50.9%
Managers of other departments (Human Resources, Legal, Operations, etc.)	59.4%
Members of senior management (such as chief executive officer, chief information officer, chief financial officer, etc.)	79.4%

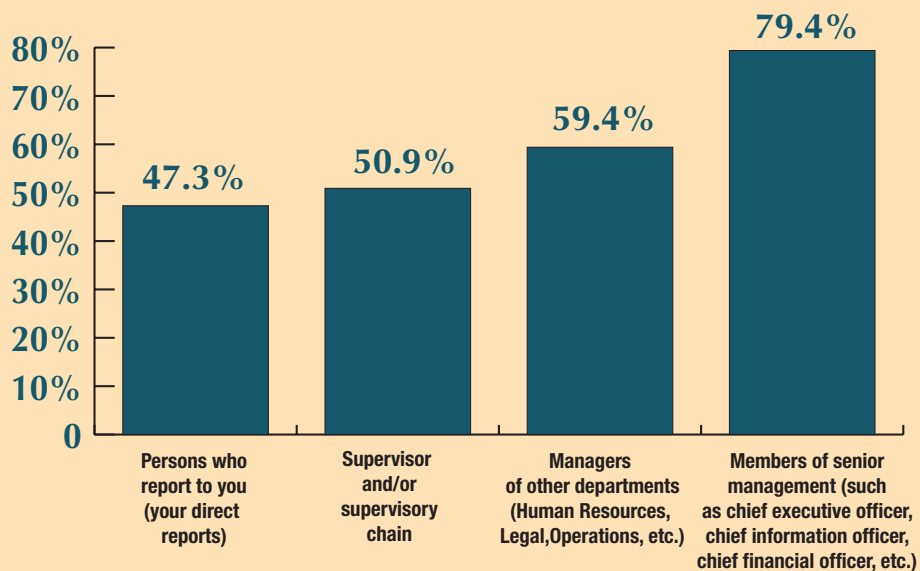## Q9: Metrics Provisions To Non-Security Persons – How Often?

9. If Security provides these metrics to persons outside the department, how often do you share the metrics?

Answer Options	Response %	Response Count
Monthly	40.1%	65
Quarterly	42.6%	69
Annually	17.3%	28
Other (please specify)		21

1) N/A
2) We are consultants. It varies with the client.
3) Upon request
4) It is provided monthly, quarterly and annually.
5) Weekly
6) Not providing to outside party
7) Some are shared weekly
8) After audits based on audit schedule
9) Also ad hoc as required and during 1-1 meetings with business leaders as appropriate
10) Varies by metric and audience
11) All depends on the customer and the measurement.
12) As needed or upon request. Not on a regular basis
13) Depends on what's been measured
14) In the future monthly
15) Both monthly and global reporting annually
16) Actually all above, but then different metrics.
17) Some metrics are also shared quarterly and annually
18) NA
19) As part of consulting assignments and sales presentations
20) With an annual review
21) AS DEEMED APPROPRIATE

9. If Security provides these metrics to persons outside the department, how often do you share the metrics?

- 42.6% Quarterly
- 40.1% Monthly
- 17.3% Annually

Legend:
- Monthly
- Quarterly
- Annually

Q10: Metric Elements Shared With C-Suite Personnel

10. If metrics are provided to C-Suite personnel, exactly what elements are shared? (Select all that apply)

Answer Options	Response %	Response Count
Guarding performance (turnover, inspections, etc.)	20.1%	31
Cost against budget	61.7%	95
Criminal incidents and investigations	56.5%	87
Security incidents	79.9%	123
Security training and education	32.5%	50
Communication and awareness programs	24.7%	38
Systems performance/ downtime (CCTV/ Access Control/ Alarm Systems)	16.9%	26
Regulatory compliance	44.2%	68
Physical security	29.9%	46
Background screening	16.2%	25
Risk analysis process	39.6%	61
Audit implications	30.5%	47
Internal customer satisfaction	21.4%	33
Other (please specify)		22

1) Response Matrix's
2) Shortage results
3) Ergo
4) Comparisons to competitors in the market as well as year over year performance
5) Losses
6) Safety according to OHSAS 18001
7) Not providing to outside party
8) We have a number of internal department metrics, but only roll up 2 to C-Suite. One is a measure of the effectiveness of our Intrusion Detection Systems (IDS) and the other is a Personnel Security Unit measure related to pre-employment background investigations.
9) Repeat findings of non-compliance with standards or performance goals
10) Cost
11) Enterprise Risks
12) Not shared directly with C-suite personnel, but they are available to them through the Security Council.
13) Incident closure time (days)
14) Cost
15) International Travel Statistics
16) Revenue protection. Business impact analysis. Crisis Management ability
17) External Fraud
18) Open shifts or Open Posts - fill-in officers sent to post, scheduling issues in general.
19) Response times to "code" calls
20) Loss rate (shrinkage)
21) Those listed previously under the same question.
22) Crisis Management preparedness

Q11: Most Important Metrics – Senior Management

11. In your organization, what elements or metrics does senior management view as the most important?

Responses	159
1) Cost and risk reduction	
2) Incidents, Budget, Regulatory	
3) Criminal incident and investigations	
4) GL and Workmen's Comp, Compliance and Security Incidents	
5) Guarding performance	
6) All	
7) Key Wins	
8) Customer Satisfaction Response Matrix	
9) Shortage results	
10) Costs against budget and compliance (physical security reviews)	
11) Risk Analysis Process	
12) Cost vs. Budget	
13) Budget	
14) Compliance and audit with budget coming in a close second	
15) Cost against budget; employee retention	
16) Cost vs. budget and security incidents	
17) All	
18) Costs, performance, and ROI	
19) Unclear	
20) Losses	
21) ISO 9001 and OHSAS 18001	
22) Compliance to standards	
23) Costs, Regulatory	
24) Budget	
25) Loss and frauds events	
26) Financial loss figures and incident trends along with regulatory criminal reporting.	
27) Budget, loss control, safety	
28) Shrink, investigative closure rates on robberies and burglaries	

29) Audit implications
30) Regulatory, budget and audit.
31) Metrics related to Key Performance Indicator and service delivery ratings.
32) Budget
33) Directness. Simplicity. Result Oriented. Safety.
34) Value verses cost.
35) Incidents
36) Budget and incident rates
37) Criminal Incidents Security Incidents Cost Against Budget
38) Return on Investment
39) Risk vs. reward
40) Budget, system performance and Internal/External Customer Satisfaction
41) Security Incidents
42) Fraud and robbery loss data
43) The effectiveness of the intrusion detection systems.
44) Audit
45) Risk and regulatory compliance issues
46) Bottom line and reputation
47) Health & Safety Security incidents last 13 months, High Potential Incidents, Incidents by Region
48) Budget
49) Cost vs. plan. Metrics where a good story can be told;
50) Cost
51) Information Sharing of Incidents, awareness and using data to provide predictive analysis for Prevention
52) Performance and cost (roi)
53) Cost, risk analysis, service delivery
54) Criminal Cost/Expense Ratio FTE justification
55) Budget vs. cost Criminal/security incidents Capital investment in security infrastructure Risk

56) Employee safety and facility security metrics.

57) Incidents

58) Threat and risks to staff and assets.

59) Employee safety and security

60) Cost (based on similar organizations)

61) Wpv

62) Incidents and Audit Compliance

63) Value Metrics: Those things that show business enablement by my organization

64) Performance goals

65) Regulatory compliance
Audit implications
Cost against budget

66) Actual vs. Budget Costs

67) Those the reveal efficiency and effectiveness measures, trends and service level agreements (e.g. cycle times for Due diligence, background investigations, regulatory response matters etc) We are in the process of developing new KPI's that are standard across all other service functions such as security costs as a percentage of company revenue, costs, per associate etc.

68) Security incidents, criminal incidents, risk analysis

69) Cost relative to services provided

70) Trends as they relate to risk & threat to our employees or operations

71) Enterprise Risks and Investigations/Incidents

72) Regulatory compliance. System performance. Customer satisfaction. Cost to budget.

73) Security incidents

74) Events that impact employees
Intellectual Property loss
Other asset losses

75) Audit Implications, and Regulatory Compliance.

76) Risk analysis process, security incidents, cost against budget

77) Varies from time to time

78) Budget, risk based metrics i.e. security incidents

79) Cost vs. budget
measurements of our new SOC

80) Incidents and mitigation

81) Overall activity and customer satisfaction.

82) Incidents

83) Cost against budget Risk analysis process
84) Cost against budget, criminal incidents and investigations
85) - Arrest, use-of-force & confinement incidents; - significant security incidents
86) Security incidents & loss
87) The ones provided
88) Security cost versus turnover
89) Internal customer satisfaction and regulatory compliance
90) Cost against budget; security incident tracking
91) Physical security, incidents
92) Budget
93) Most all with an emphasis on regulatory compliance
94) Cargo theft incidents, Crime Analysis
95) Risk exposure
96) ROI Risk (as it relates to increased insurance premiums or negative press)
97) Security incidents
98) Primarily compliance/client expectation issues such as security awareness, lost/stolen electronic devices & sensitive documents, encryption statistics, and actual expenses vs. budget.
99) Costs, incidents
100) Incident Rates
101) Security Incidents and Cost against Budget
102) Cost against Budget Security Incidents Risks analysis
103) Available resources and their optimum utilization; use of specialists for special assignments; efficiency v/s cost effectiveness; efforts and time spent on primary and secondary responsibilities.
104) Client satisfaction from the security department
105) Cost against budget
106) Legislative/Regulatory compliance, customer satisfaction and cost
107) Actual and prevention of harm incidents - robberies, assaults, etc.
108) Crime Figures relating to freight losses and crime clear up figures.
109) Information Assurance

110) Incidents, cost, compliance.
111) Cost
112) ID badge mishaps, phone calls received, arms qualified Officers, Catastrophe Duty deployment days spent by guard force personnel/and cost to the client, number of firearms certified Officers, access control measures, value added services, mobile patrol mileage and parking violations written, number and types of reports generated, tenure of various Officers in various positions.
113) Regulatory Compliance and International Travel Statistics
114) ROI, Officer / Manager retention
115) Compliance
116) Key performance indicators based on pre identified security risks relevant to the enterprise.
117) Budget
118) Always the most importance is placed on the value of the officer task or guest service in relation to cost and overall benefits
119) Not sure. But we align what we review with the organizational pillars such as protecting our supply chain.
120) Customer retention, customer satisfaction, employee turnover and profitability
121) Incidents/ crimes, BIA, RM, Revenue Protection, Regulatory compliance.
122) Product production, not security.
123) Metrics on key initiatives, compliance programs and major loss drivers
124) Hours of service provided to each client, average wage of officers, turnover, overtime
125) Risk Analysis Customer data
126) Not sure as of this time. We are just beginning our metrics roll out to "C" Suite
127) Compliance!
128) Budget; incident response
129) Important health or security incidents
130) Cost
131) How we stack-up to others in the industry

132) System downtime.
133) Costs and regulatory compliance
134) Security incidents
135) Security risk analysis within the financial services industry and cost against budget
136) Anything related to spending and impact of security costs on margin erosion. Secondly, pro-active time vs. reactive (risk assessment and range (in $$$) of solutions to mitigate the risks.
137) Cost against budget & avoidable losses (safety/security incidents & theft/vandalism)
138) Criminal, cargo theft, robbery, in/out visitors and employees, incidents, etc.
139) Guard turnover, training, and incidents occurring on site.
140) Incidents
141) That all systems are working as planned
142) Any items relating to department costs
143) Security Incidents Security Budget Security Violations
144) Criminal Incidents and General Investigations
145) Budget, staffing, and incidents.
146) Cost to budget, risk analysis
147) Cost ratio budget, incidents, and regulatory compliance
148) Internal customer satisfaction
149) Budget
150) Trending on incidents Security Infrastructure ROI Incident locations
151) Security Incidents, Physical Security, and Crisis Management Preparedness
152) Operations; Financials
153) Budget, Incidents and Customer satisfaction. We also employ Relentless Root Cause Analysis (RRCA) for incidents, issues or "turn backs;" the internal matrix that shows the 8D process is viewed by senior management as appropriate
154) Cost savings...
155) Costs, service levels and security incidents
156) Cost
157) Risk analysis process
158) The human resources.
159) INFORMATION MANAGEMENT

EFFECTIVE, EVALUATED SECURITY METRICS—© ASIS Foundation 2014

Qualitative Results: 11. In your organization, what elements or metrics does senior management view as the most important?				
	Assigned Category #1		**Assigned Category #2***	
Category:	**Response Count**	**Response %**	**Response Count**	**Response %**
Finance	60	37.7%	12	7.5%
Security Incidents/Safety Considerations	41	25.8%	17	10.7%
Risk	13	8.2%	8	5.0%
Compliance	12	7.5%	9	5.7%
Operations	6	3.8%	2	1.3%
Business Impact/Performance	5	3.1%	4	2.5%
Customer/Employee Satisfaction	5	3.1%	2	1.3%
Customer Service	2	1.3%	4	2.5%
Turnover	1	0.6%	4	2.5%
Other	14	8.8%	0	0.0%

*Note that some responses pertained to multiple categories and thus had 2 assigned categories.

Q12: Most Important Metrics – Why?

12. Why are those metrics viewed as the most important?

Responses	141
1) Implications and nexus to business operations	
2) Customer service oriented	
3) Money and Reputation	
4) Cost	
5) Why track anything that is not important?	
6) Serve as the highlight of our service	
7) Measures companies effectiveness and customer health	
8) They impact the financial performance of the company. The lower the shortage the more it contributes to the bottom line.	
9) We want to ensure we're in compliance and that we are keeping our expenses reasonable.	
10) Operational security	
11) To show the total value the department has brought into the organization for the given year in comparison to most recent historical data	
12) The money is coveted for other uses.	
13) Continued operations	
14) Financial impact on the organization's bottom line	
15) Budgetary implications and potential impact of security-related events.	
16) N/A	
17) They affect the bottom line.	
18) Loss Mitigation Performance	
19) They monitor quality, safety and security	
20) P & L, Impact to Corporation	
21) Budget	
22) Because it means money	
23) Banks are under scrutiny by regulators to report such activity and are fined when they fail to make such reports.	
24) Their impact to bottom line, reputation	
25) Indication of losses and customer/employee safety	
26) Part of the performance plan and appraisal.	
27) Because we are in a highly regulated industry	

28) These relate to our function KPIs as a whole and directly relates to ROI and contract performance by security service providers.
29) Cost efficiency
30) No Gimmicks. No credit given to showboating.
31) Measure of employee and asset protection. Also ROA for security costs.
32) Public Liability Trending Analyses Operating Expense Controls
33) Want to make sure budgets are applied effectively.
34) Establish the ability to quantify success
35) Operations effective and efficiency and Customer Service
36) Directly effects customer base
37) Financial loss and human safety
38) We know by the measurement if all our security systems are functioning properly, any failures are being addressed timely, and the systems and operators catch penetrations during testing.
39) Compliance and business process improvement
40) Larger potential impact to the entity depending on the business environment they work within
41) Money and reputation
42) Measure the effectiveness of programs in region
43) Cost Containment
44) C suite enjoys the stories around the metrics.
45) Affect P&L
46) Allows program to have best chance to succeed
47) Budgeting, determination of amount of resources needed to provide safe environment
48) They determine the effectiveness of the security program
49) Measurement of risk commensurate with costs
50) Significant number of employees and facilities.
51) The quality of metrics is poor and no other viable metrics are available.
52) Involve, people, all assets and of course funding
53) Company measures itself competitively against similar organizations under a 'private and voluntary' cost comparison.
54) Wpv
55) Personnel and asset security; regulatory compliance

56) That validate and justify the expenditures being made for our organization

57) Reflects risk tolerance

58) Compliance is very important; doing the right things the right way to avoid unnecessary penalties.

59) Organizational focus is cost management

60) They reveal the effectiveness of the organization as well as the trends that point to areas of risk, concerns or otherwise necessitate capturing the attentions of the audience.

61) Security incidents suffered by company personal, cost against budget

62) Provides business case for non-revenue function

63) There is a potential to mitigate the risk to uphold company reputation and stability

64) Risks impact the business, customer and shareholders therefore, they are the most important.

65) We are in a highly regulated environment so that is easily # 1.

66) The security and safety of our employees is paramount.

67) Company vision and competitiveness

68) Critical impact to business if left unattended. Legal liability

69) Risk based organization with tight fiscal challenges

70) Cost, being we are establishing a new program.

71) This is where the risk lies

72) Demonstrates the value add and also the reception of business leaders

73) Due to the wider implication of the event.

74) They are always looking to reduce costs
They are legally required to do risk analysis

75) They are viewed as the most important because senior management has insufficient knowledge on security issues.

76) Potential for liability and risk assessments.

77) To be under 2,5% of the turnover

78) Part of the company strategic plan

79) They are deemed to be the most critical, and to reflect a measure of ROI

80) Cost containment

81) Regulatory requirements

82) Allow to them have an approach to take decisions keeping in mind that in Mexico we have a critical security environment

83) They clearly determine return on investment.

84) It is always about the profit and corporate image

85) To focus on areas that may require improved resources.
86) We provide professional consulting services and deal with a large amount of sensitive client data. Our clients expect success in these areas, and hold us contractually to certain expectations. Various states and countries also have Privacy regulations that we are required to comply with.
87) Low level of awareness of the other security metrics
88) To assess the security / safety environment for patients, visitors and staff.
89) Reflects the success of the program
90) To evaluate Return on Security Investment; assigning the right person for the right job and optimal utilization of available resources.
91) Measurement against other department in the org
92) Always important to maintain budgetary discipline and to ensure a good balance between cost of security program and asset being protected
93) Leg/Reg is a legal must; customer satisfaction provides a comprehensive measure of how every aspect comes together to ensure we attract and retain customers and the cost aspect further completes the picture regarding contribution to shareholder value.
94) Impact upon team and cost
95) These impact on our customer satisfaction and have an impact on our corporate name.
96) Critical nature of our systems.
97) Cost
98) Customer service interactions, costs, and multi-tasking ability as technology increases, workplace protections efforts, traffic control, communication efforts, turnover monitoring and experience accrued.
99) Regs keep us open and we travel a lot.
100) Cost saving events.
101) Contract related
102) They represent overall security trends that could affect the enterprise.
103) Cost implications, cash flow
104) These two actions impact the guest, who gives us the money, if there is no clear benefit there may be a cost savings here.
105) Direct impact to our business.
106) Growing the business and profitability
107) Highest possible negative effect and good understanding of the level of ability we have to deal with unwanted events.
108) Bottom line in business.
109) Impact to the business

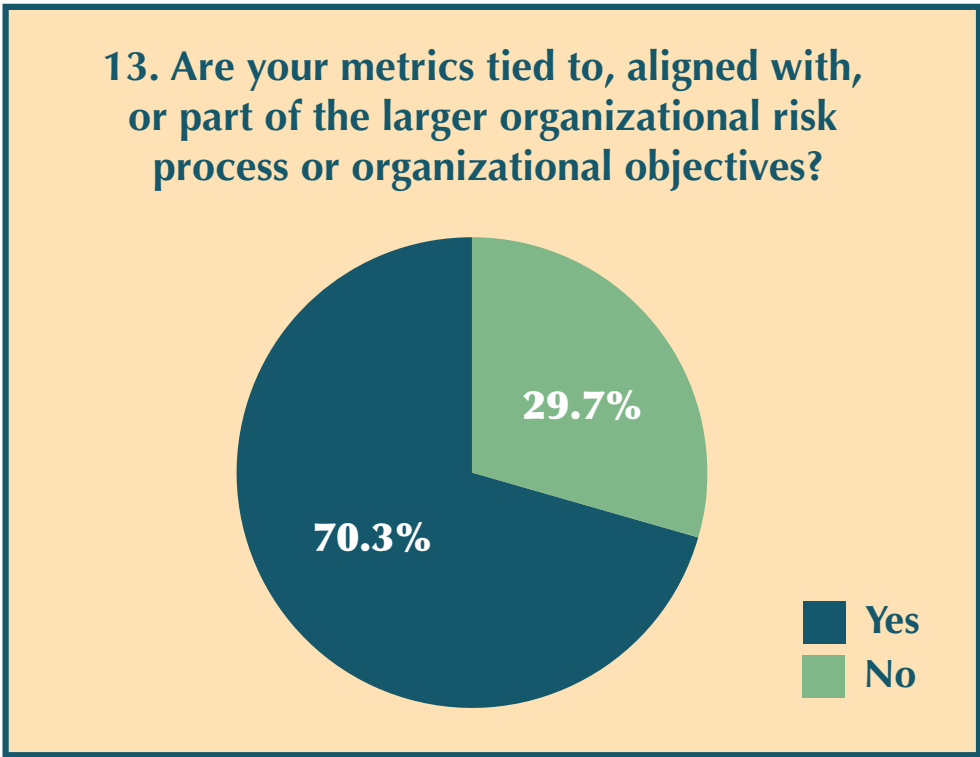| |
|---|
| 110) They are what drive the operations financially of the company. |
| 111) Safety & Security of employees |
| 112) Cost, performance and penalty implications. |
| 113) Controlling costs company wide; incidents affect safety and health standards |
| 114) Because of their legal impact |
| 115) No money |
| 116) Determines value of spending |
| 117) Determines system availability. |
| 118) Impact to business. |
| 119) Life safety implications |
| 120) These are hot topic areas in physical security within the financial services industry |
| 121) Because the impact profitability and ability of operational teams to enter markets where risks are high or extreme for a manageable cost. |
| 122) Contribute to the company bottom-line |
| 123) Because is the element that give us the tendencies. |
| 124) They impact the delivery of services to clients. |
| 125) Employee safety and satisfaction |
| 126) I have gone from having the information in my head to putting down on paper |
| 127) Alignment with the Corporate goals/objectives |
| 128) Potential media interest and impact on the organization (people, assets, information) |
| 129) These are the metrics we established in our annual management planning exercise. |
| 130) Budgets rule in this day and age and Risk can blow a budget. |
| 131) Risk to organization |
| 132) That's what generates the business |
| 133) Always about the bottom line |
| 134) Determines budget allocation justification |
| 135) Critical to business continuity |
| 136) That's where the money is. |
| 137) Budget = Bottom-line, Incidents are tangible and our organization places high value on customer satisfaction; both internal and external |
| 138) Impact to the organization and the employees |
| 139) We operate under a Risk Management process |
| 140) No system will function to its desired level without the support of the human resource. |
| 141) CONFIDENFIALITY, INFORMATION SECURITY |

Qualitative Results: 12. Why are those metrics viewed as the most important?				
	Assigned Category #1		**Assigned Category #2***	
Category: **Impact On:**	**Response** **Count**	**Response** **%**	**Response** **Count**	**Response** **%**
Finance	54	38.3%	1	0.7%
Business/Performance	27	19.1%	12	8.5%
Compliance	12	8.5%	4	2.8%
Security Incidents/ Safety Considerations	10	7.1%	10	7.1%
Risk Assessment	9	6.4%	4	2.8%
Customer Service	8	5.7%	3	2.1%
Communications	5	3.5%	2	1.4%
Operations	5	3.5%	4	2.8%
Other	11	7.8%	0	0.0%

*Note that some responses pertained to multiple categories and thus had 2 assigned categories.

Q13: Metric Alignment With Risk/Objectives

13. Are your metrics tied to, aligned with, or part of the larger organizational risk process or organizational objectives?

Answer Options	Response %	Response Count
Yes	70.3%	130
No	29.7%	55

13. Are your metrics tied to, aligned with, or part of the larger organizational risk process or organizational objectives?

29.7%

70.3%

Yes
No

Q14: Metric Alignment With Risk/Objectives – How?

14. If "Yes", how?

Responses	111
1) PCI and other compliance requirements in financial services (MTL for States, etc.)	
2) Electronic reporting	
3) We measure how Security performance from training, post coverage, etc. affect incidents, etc.	
4) Part of overall company goals, especially budget	
5) Continuous improvement program	
6) The safety of our Associates and customers.	
7) Security is tied into so many business units, from risk, business continuity, travel, crisis manment, compliance, investigations, major events, pre-employment background investigations, executive protection, intelligence analysis- so, without question, our goals and objectives are aligned with the Business.	
8) Layered security objectives	
9) We're provided with a budget each year that has certain expectations set in workplace violence, reduction in force management, executive protection, corporate investigations, etc. that directly support the company mission as well as market trends the company is following & supporting	
10) Dashboarding for systems based tracking and via weekly deliverables for all other areas/teams	
11) We prepare security assessments and recommendations. The metrics assist us in refining our data and providing better more comprehensive results.	
12) Aligned to business risk reduction	
13) Connected to ISO 9001 and OHSAS 18001	
14) Costs	
15) Security is considered one risk specialty in our Operational Risk program along with Legal risk, information security risk, HR risk, etc.	
16) Only marginally. Work is in process to create a more uniform dashboard of risk events, etc. that will roll up to executive management and the BOD.	
17) We have to report our results to the risk department which creates risk assessments for the entire business	
18) Via the yearly assurance letter of the board.	
19) We use the to show how security can help make the business more effective. Security is not just a line item expense.	
20) N/A	

21) Annual review
22) Forward planning
23) Security Metric rolls up to Operations Metric
24) To the organizations overall risk tolerance
25) Quarterly reviews and annual performance bonus tied directly to results.
26) Risk management utilizes the information for insurance.
27) Metrics are used to indicate the effectiveness of the risk mitigation and regulatory compliance program.
28) The metrics partly demonstrate how objectives are being met. The objectives are set top down. Therefore the security performance directly affect the performance of the C suite member responsible
29) Integrated into annual operational plans
30) Part of overall program to provide best opportunity for Prevention
31) Is considered on of the major risk factors for the organization
32) Direct alignment between security goals/objectives with business
33) Placed into Issues Management and Integrated Risk Management Programs
34) They are aligned with the Physical Environment section of the overall Quality of care
35) Fully integrated into ERM process
36) Tied to internal employee survey metrics and external customer survey metrics.
37) Part of the key performance indicator and risk management system.
38) Take a look at the overall framework in the Organization
39) They all link back to our Shared Services Strategies of providing effective services at an affordable cost
40) Part of company management system
41) Everything is to be aligned with the big picture: To be the industry leader and innovator. And that gets accomplished by paying attention to details, which includes compliance and managing budgets very well.
42) Loosely tied to other risk based and service functions such as AMLO, business continuity etc.
43) Yearly business plan and strategic objectives
44) In early stages of looking at the security metrics as part of the large ERM program
45) The metrics align with the company's enterprise risk metrics
46) We lead the overall company risk management.
47) They form part of the risk profile for the Company

48) Tied to Enterprise Risk Management process
49) Performance management
50) Safety and security of our patients and staff is a strategic priority
51) Especially around management of aggressive behavior/violence
52) Information sharing and cross audits
53) Through a risk assessment process and mitigation actions.
54) Risk reduction work in all departments
55) The program related to operational risks is developing on a priority basis.
56) TRIM based measurement
57) By global risk analysis
58) Included in the organization strategic plan
59) The internal security metrics are tied to broader KPIs
60) Multiple government organizations
61) Need to show how they contribute to the overarching company goals.
62) Aligned with the corporate goals and objectives
63) It is part of the business in order to take decisions according with the Risk Level
64) Roll up to overall global risk exposure and mitigation that feeds into shareholder expectations.
65) To the overall security of the organization
66) Our metrics are tied to the company's overall client satisfaction levels and we want to view them as a difference maker between our competitors and us. All other things equal, if we are more secure than our competitors that will improve business. Because some of our metrics address contractual obligations and some address regulatory, we also work closely with our Legal Dept. and various Business Units.
67) They indicate how the Security function is contributing to providing a secure/safe environment for the patients, visitors and staff.
68) The security goals derives from the business plan
69) Half a year company and plants general risks analysis
70) It's part of the overall review at the highest level with common metrics.
71) It's often aligned with OIMS.
72) In contributing to the overall organizational risk management profile, what risk is accepted and the potential for impact on business objectives
73) Safety and operations teams

74) Security ultimately reports to the General Manager of Global Compliance. Security figures are used in forming internal audit procedures and measures.

75) Alignment with annual goals.

76) Risk manager

77) Security is a business function, and thus, tied into the bottom line of the enterprise.

78) Some contracts require greater security controls.

79) Enterprise risk needs to be identified in order to measure what metrics would be relevant to the risk owners. We've interviewed many members of Sr. Management to get to this point.

80) Risk Assessments are conducted every 3 years with benchmarking yearly against competitors. The overall corporate strategy and plan the final tally of where or whether cuts can be made.

81) Program protects our most successful product line(s).

82) BCM is tied to the IPO (stock exchange). Crimes are tied to our strategy to be the best and most secure player on the market.

83) By being rolled up into sub groups

84) Financial and regulatory

85) As a private security company, providing security officers to large corporations by contract, understanding the performance of the contract is what drives our business practices.

86) Global risk analysis

87) Finance, enterprise risk, legal, compliance.

88) Aligned with budgetary controls at company level

89) Supports the organization's business plan.

90) Costs related to EBITDA

91) Tied as related to broader risk assessment and avoidance.

92) Total functional spend of the enterprise.

93) To better protect and prevent any risk our organization.

94) Annual risk management surveys.

95) Material we provide to auditors, they love to see backup and paperwork.

96) Some of the metrics are security inputs into the overall corporate goal.

97) We are part of the organizations Integrated Risk Management process

98) Same risk model

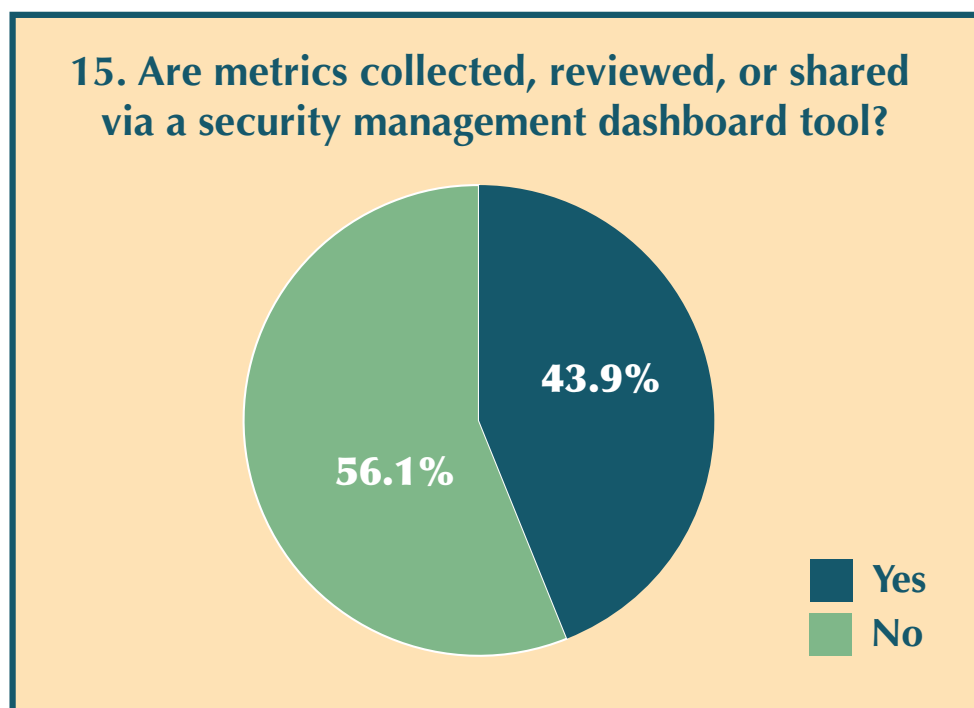| |
|---|
| 99) The top management of the hospital sets broad goals. Management plans are written to achieve the goals of the organization. At the end of the year performance indicators established in management plans are used to determine the level of achievement of the management plans and their implication on the organization's overall plan. |
| 100) Metrics from each site are benchmarked against the division, region and company to determine a base standard from which to work. |
| 101) Compares to the risk management and IT risk compliance factors for continuity of business rations |
| 102) It helps to retain clients |
| 103) Metrics are aligned with overall strategic objectives and criticality of business continuity |
| 104) Enterprise Risk Management process |
| 105) We conduct an Enterprise Risk Management assessment; this sets some baselines for measures |
| 106) Track back to Company's annual risk assessment areas. |
| 107) Part of our risk assessment program includes various metrics as a way to determine protection levels |
| 108) Budget |
| 109) Top 25 Public Universities - Efficiency & operation |
| 110) To assist in providing adequate security coverage. |
| 111) IS ANCHORED BY OTHER RELATED DEPARTMENTS |

Qualitative Results: 14. If "Yes", how?				
	Assigned Category #1		**Assigned Category #2***	
Category: Aligned with:	**Response Count**	**Response %**	**Response Count**	**Response %**
Risk	40	36.0%	2	1.8%
Objectives/Goals	11	9.9%	1	0.9%
Finance	9	8.1%	4	3.6%
Annual/Future Plans	8	7.2%	2	1.8%
Security Incidents/Safety Considerations	7	6.3%	0	0.0%
Reports/Reviews	7	6.3%	1	0.9%
Performance	7	6.3%	1	0.9%
Compliance	5	4.5%	4	3.6%
Operations	3	2.7%	3	2.7%
Customer/Employee Focus	3	2.7%	0	0.0%
Other	11	9.9%	0	0.0%

*Note that some responses pertained to multiple categories and thus had 2 assigned categories.

Q15: Dashboard Tool Usage

15. Are metrics collected, reviewed, or shared via a security management dashboard tool?
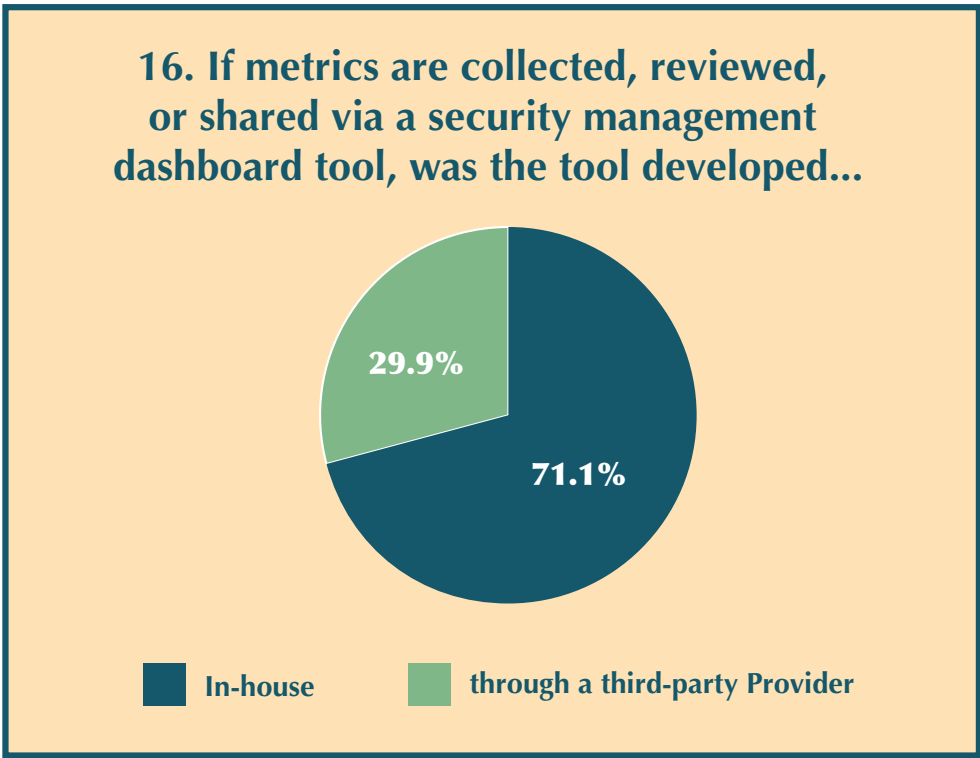
Answer Options	Response %	Response Count
Yes	43.9%	82
No	56.1%	105

15. Are metrics collected, reviewed, or shared via a security management dashboard tool?

43.9%

56.1%

Yes
No

Q16: Who Developed Dashboard Tool?

16. If metrics are collected, reviewed, or shared via a security management dashboard tool, was the tool developed...

Answer Options	Response %	Response Count
In-house...	71.1%	59
Through a third-party provider	28.9%	24

16. If metrics are collected, reviewed, or shared via a security management dashboard tool, was the tool developed...

29.9%

71.1%

■ In-house   ■ through a third-party Provider

Q17: Third-Party Dashboard Tool Name

17. If the dashboard tool is from a third-party provider, what is the tool's name?

Responses	35
1) N/A	
2) ECM. It is a case management system developed in partnership with a third party vendor.	
3) N/A	
4) Archer	
5) D3	
6) Archer	
7) In-house	
8) Our clients use multiple products	
9) TIPS (Threat assessment, Incident management & Prevention Services) from Awareity	
10) Archer	
11) Not free to disclose	
12) Perspective / Focal Point	
13) Archer	
14) Also use reporting tools from CESI (ReportExec) and DNV audit tools	
15) Synergy	
16) N/a	
17) Decline	
18) Syrus	
19) N/a	
20) N/A	
21) MIST	
22) Archer	
23) We call it Security Incidents Trend Summary. It may with a different name in some other organizations.	
24) Perspective - for dealing with incidents, investigations and some project time investments	
25) Archer	
26) MS-Shift	
27) Guard services group is out sourced so as a part of that service the vendor provides a dashboard, which also tracks our key performance indicators.	
28) N/a. Developed in house via a third party platform.	

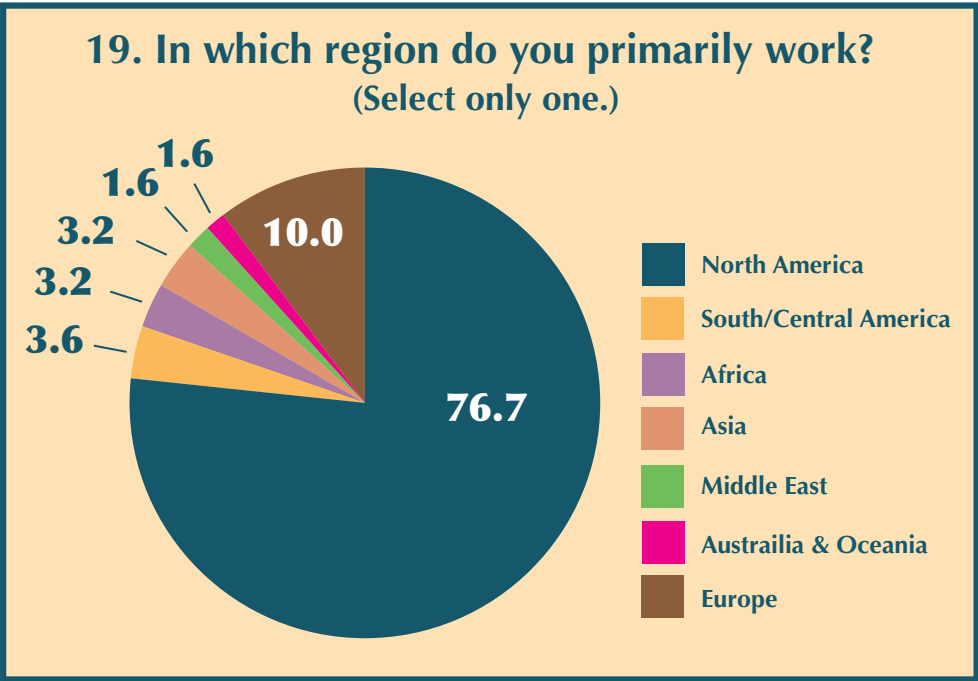| |
|---|
| 29) NA |
| 30) All the news, government statistics and private companies |
| 31) Supplier own (G4S) |
| 32) 3D Security Management |
| 33) MS Shift |
| 34) N/A |
| 35) ISO 27001 |

Q18: Metrics Interview Volunteers – Contact Information

18. The ASIS Foundation Security Metrics Research Project is trying to identify specific metrics and develop a way to assess their validity. If you are using metrics, would you be willing to speak briefly with a researcher? If so, please provide contact information. Your support in this effort is absolutely vital for the ASIS Foundation Security Metrics Research Project.

Answer Options	Response Count	Response%
Name:	91	100.0%
Title:	90	98.9%
Organization:	90	98.9%
Email Address:	88	96.7%
Phone Number:	80	87.9%

Respondents' names and contact information have been redacted from this report.

19. In which region do you primarily work? (Select only one.)

Answer Options	Response %	Response Count
Africa	3.2%	8
Asia	3.2%	8
Middle East	1.6%	4
Australia and Oceania	1.6%	4
Europe	10.0%	25
North America	76.7%	191
South and Central America	3.6%	9

Q20: Desire Information Regarding Metrics – Contact Information

20. If you would like to receive information from ASIS regarding metrics, please supply your...

Answer Options	Response %	Response Count
Name:	100.0%	164
Email Address:	99.4%	163

Respondents' names and contact information have been redacted from this report.