The use of metrics to manage enterprise security risks: Understanding, evaluation and persuasion

Peter E. Ohlhausen* and Daniel McGarvey**

Received (in revised form): 6th April, 2018

*Ohlhausen Research, Inc., 8803 Prudence Drive, Annandale, VA 22003, USA
E-mail: peter@ohlhausen.com

**Alion Science and Technology, 4300 King Street, Alexandria, VA 22302, USA
E-mail: dmcgarvey@alionscience.com

Peter E. Ohlhausen is a researcher and consultant in security, criminal justice and technology. As President of Ohlhausen Research, Inc., he performs security and crime-related projects for corporate clients and such organisations as American Society for Industrial Security International (ASIS International), John Jay College of Criminal Justice, US Department of Justice, US Department of Homeland Security and the International Association of Chiefs of Police. He was formerly editor of Security Management, the monthly magazine on corporate security. He was a speaker at the ASIS Annual Seminar & Exhibits from 2013 to 2017. Mr Ohlhausen graduated from the University of Virginia and has also pursued studies at Cambridge University and Harvard University.

Daniel McGarvey is the Senior Principal Business Process Analyst for Alion Science and Technology. His responsibilities include providing executive consulting in strategic planning for programmes supporting government and industry. He is the Senior Instructor for the National Security Training Institute, and the lead for analytical development in the Insider Threat Working Groups for both ASIS International and the Intelligence and National Security Alliance. He is a retired member of the Defense Intelligence Senior Executive Service, as the Director, Information Protection, Office of the Administrative Assistant to the Secretary of the Air Force, Headquarters US Air Force. He was the subject matter expert for the ASIS Foundation Metrics Research Project.

ABSTRACT

Metrics drive business decisions and behaviour. Properly developed using psychometric principles, metrics provide a solid rationale for senior management to make prudent decisions about organisational growth as well as facilitating the assessment of internal policies and programmes. Until recently, there has been little research on the development of effective performance metrics, especially in the security field. The American Society for Industrial Security International (ASIS International) provided funding for an extensive study into the development of metrics for the security profession. The study included an online survey, telephone interviews, and a review of the literature and best practices of past research on metrics. Based on the data collected, a security metrics evaluation tool was developed, incorporating core psychometric principles and reflecting both operational and strategic corporate requirements. Finally, guidelines were developed for presentation to senior executives.
INTRODUCTION

According to a well-known definition of metrics:

‘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 paper focuses on physical security, but its advice also applies to information technology security, a field in which the use of metrics is especially advanced.

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. The term ‘metrics’ is sometimes used interchangeably with ‘measurements’, ‘analytics’ and ‘performance metrics’.

At the 2017 American Society for Industrial Security (ASIS) International Seminar and Exhibits in Dallas, the authors gave a presentation titled ‘Use metrics dashboards to manage enterprise security risks’. Along with colleague Richard Weaver, Chief Security Officer, Johns Hopkins University Applied Physics Laboratory, the authors explained the purpose of metrics, summarised past and present research on metrics, described how to use a metrics evaluation tool to improve one’s metrics, and offered advice on presenting metrics persuasively to senior management.

Dashboards are popular, and they can be powerful and persuasive, but they occur at the end of a process, not the beginning. Ideally, the security professional will take steps in this order:

1. Understand the concept of security metrics.
2. Evaluate, refine and learn from particular metrics.
3. Persuasively present metrics to senior management.

Dashboards may be useful tools in steps 2 and 3.

BACKGROUND ON METRICS

Metrics drive business decisions and behaviour. They influence process assessment and controls, business policies, collaboration for enterprise-wide benefits, business investment decisions and strategic and profit centre alignment.

Metrics allow organizations to hold individuals accountable for specified results and goals, and they are a vehicle through which security programmes can demonstrate their measurable impact on an organization’s strategic, organisational, financial and operational risks and profits.

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. 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, partnered with Ohlhausen Research, to carry out
The use of metrics to manage enterprise security risks

The research resulted in a detailed report titled ‘Persuading Senior Management with Effective, Evaluated Security Metrics’, which is free to download from the ASIS website. This paper includes and expands on themes from that report.

The project report presents detailed findings, including the project’s 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; and
- guidelines for the effective use of security metrics to inform and persuade senior management, with an emphasis on organisational risk and return on investment.

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

- Review and summarise literature on the use of security metrics to inform and persuade corporate management. The review cites approximately 100 sources.
- Develop and refine a 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, each evaluated by three reviewers using the Security MET.
- Develop guidelines for the effective use of security metrics to persuade senior management. The guidelines were based on a variety of sources: the literature review, the online survey, the follow-up telephone interviews, the advisory board and the expert panel.

EVALUATION TOOL

The 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, organisational 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 the report ‘Persuading Senior Management with Effective, Evaluated Security Metrics’.

The tool was developed through a lengthy, iterative process that involved synthesising scientific literature, security industry standards, and input from metrics experts on 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 tool includes the following criteria for evaluating a security metric:

- **Technical criteria — Category 1:**
  1. reliability;
  2. validity;
  3. generalisability.
Operational (security) criteria — Category 2:
(4) cost;
(5) timeliness;
(6) manipulation.

Strategic (corporate) criteria — Category 3:
(7) return on investment;
(8) organisational relevance;
(9) communication.

For each criterion, the Security MET presents a definition, concept illustration, behaviour summary scale and sample applications to help users understand how to evaluate the metric. Lower scores on particular criteria show where a metric has room for improvement. The Security MET establishes a common frame of reference for metrics users to employ when examining and rating their metrics.

Figure 1 shows how the Security MET presents one of the nine criteria, organisational relevance.

In Figure 1, the concept illustration, using object weight, is a simplified example to explain the notion of organisational relevance, based on notions from psychometrics and measurement theory.

Psychometrics is the field concerned with the measurement of mental traits, abilities and processes. There are several

---

**Criterion 8: Organisational relevance**

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

Illustration of the concept:

An organisation 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 organisational 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 organisational 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 organisational relevance, 5 = high organisational relevance

1

(1) The metric is not linked to a specific organisational strategic mission, objective, goal, asset, risk, threat, or vulnerability; if linked, the linkage is weak and of minimal relevance to the organisation; the data derived from this metric is of little importance to senior management.)

2

(2) The metric is somewhat linked to a specific organisational strategic mission, objective, goal, asset, risk, threat, or vulnerability; the linkage is moderate and of some relevance to the organisation; the data derived from this metric is of some importance to senior management.)

3

(3) The metric is explicitly linked to a specific organisational strategic mission, objective, goal, asset, risk, threat, or vulnerability; the linkage is strong and of high relevance to the organisation; the data derived from this metric is of great importance to senior management.)

4

(4) The metric is explicitly linked to a specific organisational strategic mission, objective, goal, asset, risk, threat, or vulnerability; the linkage is strong and of high relevance to the organisation; the data derived from this metric is of great importance to senior management.)

5

(5) The metric is explicitly linked to a specific organisational strategic mission, objective, goal, asset, risk, threat, or vulnerability; the linkage is strong and of high relevance to the organisation; the data derived from this metric is of great importance to senior management.)

---

Figure 1 Example of how the Security MET presents the criterion of organisational relevance
reasons why the psychometric literature is particularly applicable to developing and maintaining security metrics. In particular, the psychometric literature addresses the measurement of complex human behaviours, including the various sources of error inherent in social and organisational 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.

Taking the concept to the next level, a simplified illustration of how to apply the organisational relevance criterion in the security field is as follows. Suppose 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 per cent of the time. Therefore, a metric regarding the number of denial-of-service attacks thwarted through security efforts would be highly relevant to the organisation’s goals and would likely be of interest to senior management. As a result, the metric would receive a 5 on this criterion.

Here is a brief evaluation of a real-life metric discovered during the research. At a major financial services firm in the Midwestern USA, the vice president for security developed a metric to track 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 a phenomenon known as ‘Apple picking’ — the theft of mobile phones by criminals who grab phones out of users’ hands. At the company’s downtown office sites, a severe rash of phone theft developed. Employees were victimised on the pedestrian areas 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 exactly, and when. Using such 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 behaviour 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.

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 vice president for security reports this metric and related data to senior management every quarter to show the value of the security programme.

As noted earlier, the Security MET helps security professionals identify the strengths and weaknesses of a given metric. However, evaluating the cost of a metric (Criterion 4) may be more complicated than it first appears. Working through the Security MET process may uncover previously unconsidered costs that need to be addressed. For example, the security director of a 500-site chemical corporation began tracking the percentage of completed guard tours at each site. Each completed tour was a step toward securing the site, providing guards with an opportunity to detect and mitigate security and safety risks. By using the metric, guards were encouraged to complete their tours in a timely manner. However, analysis of the metric via the Security MET brought a concern to the surface. Criterion 4 encourages practitioners to consider the ‘the monetary and non-monetary costs associated with metric development and administration, as well as negative consequences associated with the metric’. That reminder raised serious questions. Does measuring the percentage of scheduled guard tours that were completed accidentally discourage guards from stopping to address security and safety risks that they discover? Do the guards feel they will be rewarded more for completing tours or for discovering and addressing problems, even if doing so will mean they do not finish a particular tour? In this case, the Security MET process uncovered a potential unintended negative consequence of the metric, a consequence that could be remedied through policy and training.

PRESENTING METRICS TO SENIOR MANAGEMENT

The ASIS Foundation research project noted the following:

‘Corporate management tends to view security as overhead (ie 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 with 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.’

What would make those presentations more compelling? Several key recommendations emerged from the research and from ongoing work by the Metrics Working Group:

• present metrics that are aligned with the organisation’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.

Align with organisational objectives and risks

Before choosing a metric, ‘security professionals should identify the data that is most important to senior management; metrics
The use of metrics to manage enterprise security risks

should be selected and communicated in accordance with the data that is of most importance to the audience”.7

Experts advising the researchers emphasised the importance of focusing metrics on organisational risks and objectives, as well as any other issues of importance to senior executives. Moreover, 70 per cent of online survey respondents reported that their metrics were aligned with their organisation’s risk process or objectives. One respondent explained: ‘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 organisation’s overall objectives, the security professional should focus metrics on risk and return on investment (ROI).

Risk

Survey respondents and interviewees offered insights regarding the use of security metrics to address an organisation’s risk. These are some of their comments:

- ‘We are part of the organisation’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 organisation 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.’

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.8,9 Unfortunately, calculating ROI is not straightforward, particularly in the security realm.10 However, when available, ROI data can be a great tool to harness management attention and action.

Interviewees who participated in the research offered the following insights into how they used metrics to show a return on the organisation’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 programme 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, ROI, or overall organisational 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 the information in a management context.

Present metrics that meet measurement standards

In its literature review, the research noted that ‘grounding metrics in the principles of measurement is crucial in capitalising on the benefits of metrics’.11

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.’

Tell a story

As the ASIS Foundation project report12 observes:

‘Communicating metric value remains a challenge. It does not matter how great the data is if it cannot be understood by key stakeholders.13 … 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? Security professionals can best explain their findings by providing specific, concrete examples that are meaningful to the audience.

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 organising and discerning meaning from data (i.e., trends analysis) faster and less burdensome. Sometimes metrics can facilitate creative (not fictional) storytelling. For example, a loss prevention manager at a 45-site retail operation knew intuitively that spending on remotely controlled technology (access control systems, video, data collection, intrusion alarms and safes) was worthwhile. However, he found it difficult to prove the value of those systems as not all security benefits are easily quantified. His solution was to create a new metric that recognised one of his company’s core values, namely stewardship. The new metric — reduction in the labour costs and other expenses of sending headquarters security personnel to retail locations to perform investigations and various security services — demonstrates the financial benefit of using technology solutions. Thus, by using the new metric, it was possible to present senior management with clear data showing the costs saved through the use of remote security systems.

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

**Use graphics, and keep presentations short**

The effectiveness of a metrics presentation has not only to do with content but also with presentation style. The project’s advisers 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 programme. 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 ten 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 five 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 summarise our findings and do not bother executives with trivial information. “Risk charts” resonate with senior management. We show the probability and severity of potential events and then present our risk mitigation strategy.’

**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 per cent did so monthly, 43 per cent quarterly, and 17 per cent 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 per cent of security professionals who share metrics outside the department do so at least quarterly. As data age, the information 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.

**CONCLUSION**

In sum, metrics help security professionals make informed decisions regarding their risk mitigation efforts. Metrics are also useful in conveying the value of security operations to senior management in business and financial terms they may find compelling. Carefully developed and evaluated metrics provide a sound basis for understanding security issues and free all parties (security management and senior management) from relying solely on intuition.

Ideally, the security professional will begin by learning about the concept of security metrics. The ASIS-funded research report ‘Persuading Senior Management with Effective, Evaluated Security Metrics’ is a good place to start. An important next step is to evaluate current or prospective metrics in an objective, tested fashion, such as by using the security metrics evaluation tool, and then to revise the metrics as appropriate. Revised metrics will be stronger in technical, operational and strategic terms. Once effective, evaluated, refined metrics are in place, they can be more persuasively presented to senior management, especially if the security professional employs techniques discovered in the aforementioned metrics research. The result of due attention to metrics is a more objective and scientific approach to security management.

**REFERENCES**

(4) Ibid., ref. 3.
(5) Ibid., ref. 3.


(11) Dix, J. (2013) ‘Big data the security answer?’, available at:


(12) Ohlhauen et al., ref. 3 above.

(13) Dix, ref. 11 above.

