WHITEPAPER

METRICS AND ANALYSIS IN SECURITY MANAGEMENT

By Brian McIlravey, CPP
and Peter Ohlhausen

About the Authors:

Brian McIlravey, CPP, is Co-CEO of PPM 2000 Inc. (www.ppm2000.com) and is responsible for driving strategic planning and product direction. He is a member of ASIS International's Information Security Technology Council and has experience in both corporate security and public law enforcement.

Peter Ohlhausen is president of Ohlhausen Research, Inc. (www.ohlhausen.com), which for more than 20 years has provided research and consulting to the security, technology, and criminal justice fields. He formerly served as editor of Security Management, the monthly magazine of ASIS International.

Published by PPM 2000 Inc.
www.ppm2000.com

For over twenty years, PPM has worked with organizations around the world—using their knowledge of risk management, security management and loss prevention—to provide high quality subject matter expertise in the design and application of Incident Reporting and Investigation Management software. Thousands of organizations have implemented a PPM solution, and the company's clients span all industries and the Fortune 1000. PPM is recognized by Microsoft as a Gold Independent Software Vendor.

From incident reporting, to investigation management, to actionable business intelligence, PPM offers end-to-end Incident Management solutions for—and from—security professionals. For more information on Perspective by PPM 2000, contact PPM toll-free at 1-888-776-9776 or email information@ppm2000.com.

Copyright © 2012 PPM 2000 Inc.

Contents

PPM 2000 Inc.

10088 - 102 Avenue, Suite 1307 • Edmonton, Alberta • T5J 2Z1

1-888-776-9776 • information@ppm2000.com • www.ppm2000.com

Executive Summary

The use of metrics and analysis (MA) is a sophisticated practice in security management that takes advantage of data to produce usable, objective information and insights that guide decisions. In addition, MA provides chief security officers (CSOs) with clear evidence of their operations' value, expressed in the language of top management.

As Carnegie Mellon University notes, "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."

Through MA, a CSO or other security professional can better understand risks and losses, discern trends and manage performance. He or she can also report clearly and accurately to executive management. These uses of MA all work to support the organization's strategic goals.

Software designed specifically for the security field can make the gathering of security and risk-significant data orderly, convenient and accurate—and hold the data in a format that facilitates analysis. Security and risk-focused incident management software offers both the standardization and consolidation of data. Such software also automates the task of analysis through trending and predictive analysis and the generation of customized statistical reports.

This paper synthesizes the current MA literature in the security management field. It describes the use of metrics and analysis to:

- Improve decision making;
- Strengthen security operations; and
- Gain support for the security and risk management operation.

It then describes the process of developing specific metrics, collecting and managing data and performing useful analyses with security risk-focused software.

The Power and Importance of Metrics and Analysis

This paper examines key themes and thinking in the field of metrics and analysis (MA), focusing on applications in the domain of security management. The aim is to inform security professionals about a powerful practice that is becoming increasingly essential in competitive business environments—and, in fact, is often demanded by executive management.

The use of MA is part of a serious approach to security management. In contrast to more casual, gut-oriented approaches to security decision making, MA takes advantage of data to produce usable, objective information and insights that guide decisions. In addition, MA provides CSOs with clear evidence of their operations' value, expressed in the language of top management.

The Systems Security Engineering Capability Maturity Model, developed by a team headed by Carnegie Mellon University to advance security engineering, provides an especially clear view of metrics:

> At a high level, metrics are quantifiable measurements of some aspect of a system or enterprise. For an entity (system, product, or other) for which security is a meaningful concept, there are some identifiable attributes that collectively characterize the security of that entity. Further, a security metric (or combination of security metrics) is a quantitative measure of how much of that attribute the entity possesses…
>
> 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. They are useful to senior management, decision makers, users, administrators, or other stakeholders who face a difficult and complex set of questions regarding security, such as:
>
> - How much money/resources should be spent on security?
> - Which system components or other aspects should be targeted first?
> - How can the system be effectively configured?
> - How much improvement is gained by security expenditures, including improvements to security processes?

WHY USE METRICS?

Metrics and analysis provides CSOs with clear evidence of their operations' value, expressed in the language of top management.

"What's the benefit of using metrics? Basically, to improve overall security and reduce costs."

Raymond Musser, CPP
Vice President, Security
General Dynamics
(Musser, 2011)

- How do we measure the improvements?
- Are we reducing our exposure?

The MA approach results in business intelligence, which has been defined as (PPM 2000 Webinar, 2009):

> The collection, integration, analysis, interpretation and presentation of business information to provide historical, current and predictive views of business operations, [and] the use of this information through extraction, analysis and reporting to support better business decision making.

The insights and findings a CSO gains through MA can support activities both inside and outside the corporate security department. Inside the department, the CSO can better understand risks and losses, discern trends and manage performance based on actual measurements. Outside the department, the CSO can report clearly and accurately to executive management. Both the internal and external uses of MA work to support the organization's strategic goals.

The related concept of benchmarking—comparing one's organization with others in the same industry—relies in part on using metrics. That comparison relies first of all on an understanding of one's own organization, and that understanding must be developed through MA. According to Hayes and Kotwica (2011),

> Business leaders recognize benchmarking as a proven business practice that can identify competitive strengths and vulnerabilities as well as opportunities for improvement… But while the demand for performance measures has trickled down to the security function, the appreciation for them hasn't always come along for the ride. Too many security leaders create or find benchmarks for the sole purpose of appeasing their bosses rather than from an earnest desire to use these tools to explore what others are doing, address potential gaps and add value.

It is important to remember that MA consists of both metrics and analysis. Hayes and Kotwica emphasize that point with the example of benchmarking on corporate ethics hotlines. The benchmark report may suggest that the average organization of a certain size and industry receives eight to nine calls to the corporate ethics hotline per thousand employees. If a particular company receives only three calls per thousand employees, analysis is warranted. Does the company have fewer ethics problems than its peers? Are employees intimidated into not reporting their concerns? Is the hotline underpublicized?

ALIGN STRATEGY AND PERFORMANCE

[C]orporate performance metrics… [was] the topic tackled by the most recent Blue Ribbon Commission at the National Association of Corporate Directors (NACD).

Why corporate performance metrics? Because they link corporate strategy and corporate performance…

Strategy is about the future, performance is about the past and metrics align the two.

Financial Executive (Daly, 2011)

In the MA approach, which is relatively new, key terminology is not completely settled. On one hand, Payne (2006) observes:

> *Measurements* provide single-point-in-time views of specific, discrete factors, while *metrics* are derived by comparing to a predetermined baseline of two or more measurements taken over time. Measurements are generated by counting; metrics are generated from analysis. In other words, measurements are objective raw data and metrics are either objective or subjective human interpretations of those data.

In *Security Metrics Management: How to Manage the Costs of an Assets Protection Program,* Kovacich and Halibozek (2005) define a metric as "a standard of measurement using quantitative, statistical, and/or mathematical analyses." In their taxonomy, a security metric is,

> The application of quantitative, statistical, and/or mathematical analyses to measuring security functional costs, benefits, successes, failures, trends and workload—in other words, tracking the status of each security function in those terms.

On the other hand, the National Institute of Standards and Technology (2008) states that "while a case can be made for using different terms for more detailed and aggregated items, such as 'metrics' and 'measures,' [this report] standardizes on 'measures' to mean the results of data collection, analysis, and reporting." The same source refers to the process of data collection, analysis and reporting as "measurement." *Harvard Business Review* refers to *analytics* rather than *metrics and analysis* (Davenport & Harris, 2010). The terminology will likely continue to evolve.

Despite the clear value of MA, one source suggests that only about a third of CSOs collect and analyze metrics (Kohl, 2009). Specifically, in a survey by the Security Executive Council (SEC), only 31 percent of survey respondents "gather security program data in order to create statistical reports to present to senior management."

Regarding the significance of that finding, Kohl quotes SEC spokesmen as follows:

> [I]t should be more than a wake-up call that 69 percent said they don't collect information—it should be an alarm... [A] large percentage didn't collect data because management hadn't asked for it. That... may mean management isn't even aware that security has metrics that may impact the business, or it

MAKE BETTER DECISIONS

Analytics: Using data and quantitative analysis to support decision making.

Benefits:

- Decisions are more likely to be correct.
- The scientific method adds rigor.

Caution:

- Correct assumptions are crucial.

If you don't assess the results of your changes, you're unlikely to achieve better decisions.

Harvard Business Review (Davenport, 2009)

> may mean that security is being left out of the mainstream of the organization... [S]ome security managers don't know what metrics are or how they should gather or report metrics, and that will require some training and education. [O]ther security managers feel that collecting metrics is more work than they want to do, [but if] your management has an interest or develops an interest in this area, you'd better be ready to respond.

The practice of MA is more advanced in the field of information technology security than in the field of corporate security as a whole. Although much of the research conducted so far on MA has been focused on IT, a growing interest in studying MA's application to security management is evident in an expanding focus on the subject in security conferences and publications. This paper synthesizes the current MA literature primarily in the security management field and also adds insights from more foundational IT MA sources.

The sections that follow address six key aspects of this management tool:

- Fortified Decision Making
- Metrics as a Security Operations Tool
- Metrics as Marketing for the Security Program
- Developing Specific Metrics
- Essential Ingredient: Data
- From Data to Information: Analyzing Metrics

The paper then presents recommendations on how to start employing metrics and analysis in security. A list of sources for additional information concludes the paper.

Fortified Decision Making

How can security managers make decisions that are more likely to lead to success? What, specifically, leads to better decisions? In the *Harvard Business Review*, Davenport and Harris (2010) report results from their study of 400 companies in 35 countries and 19 industry sectors.

They found that "better decisions emerge when companies systematically:

- Identify their critical decisions.
- Inventory those decisions that require analytical help.

How can security managers make decisions that are more likely to lead to success? What, specifically, leads to better decisions? In the Harvard Business Review, Davenport and Harris (2010) report results from their study of 400 companies in 35 countries and 19 industry sectors.

They found that "better decisions emerge when companies systematically:

- Identify their critical decisions.
- Inventory those decisions that require analytical help.
- Intervene where needed.
- Institutionalize what was learned."

- Intervene where needed.
- Institutionalize what was learned."

Emphasizing the "analytical help" mentioned in the second step, the authors note that "those who view analytics as just reporting on past performance don't understand the full scope and value of analytics."

Analytics, they explain, has descriptive, predictive and prescriptive properties. Descriptive analytics describe past performance. Predictive and prescriptive analytics examine data to determine significance:

> Predictive analytics—which include forecasting, predictive modeling, and optimization—are focused on the future. The use of predictive analytics takes an organization to a higher degree of intelligence and can yield competitive advantage.

Thus, analytics based on metrics, which this paper refers to as MA, appears to be an essential, foundational step in optimal decision making.

Metrics as a Security Operations Tool

Metrics and analysis (MA) can guide decisions regarding security operations in both specific and general ways. For example, at Delta Air Lines, MA is used to guide policy making. According to Kim Hodgkin, Delta's Manager of Security Administration, the company tracks compliance issues, accidents, medical emergencies, financial crimes and other losses. He notes, "Based on our metrics and analysis, we make recommendations to security leadership and other divisions." Changes suggested by MA include improved employee training, changes to screening methods, security awareness messages, and targeted investigations (Hodgkin, 2011).

Similarly, Treece and Freadman (2010) describe the use of metrics and analysis at the Massachusetts Port Authority (Massport) to solve the specific problem of security door alarms. They report that Massport greatly reduced such alarms through the analysis of alarm metrics. That analysis helped security management "determine the cause of each type of alarm and develop solutions to eliminate or reduce them." Analysis of detailed door transaction data, including video, showed the causes of alarms. That understanding led to a variety of corrective

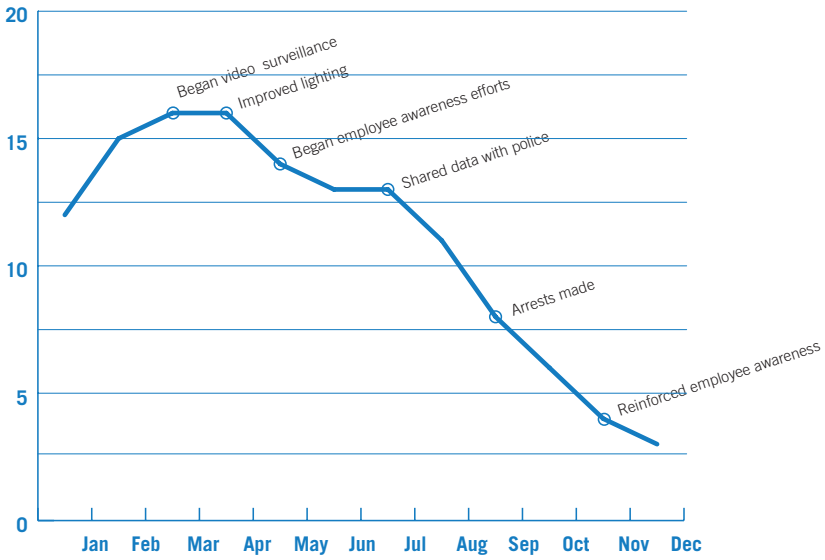
"Predictive analytics—which include forecasting, modeling, and optimization—are focused on the future. The use of predictive analytics takes an organization to a higher degree of intelligence and can yield competitive advantage."

Harvard Business Review (Davenport & Harris, 2010)

actions, including maintenance and user training. The authors report, "The result has been fewer false alarm police dispatches, which results in a more efficient use of this valuable law enforcement and security resource."

MA can be used not only to identify security problems but also to gauge the effectiveness of various security measures used to counteract those problems. For example, the chart below shows the correlation between the execution of various security countermeasures and the number of thefts from vehicles:

Effect of Security Measures on Thefts from Vehicles



MA can also be used to guide more general decisions and answer big-picture questions for security management, executive management and others. Campbell (2006a) identifies several questions that can be answered with metrics:

- How much money/resources should be spent on security?
- Which system components or other aspects should be targeted first?
- How can the system be effectively configured?
- How much improvement is gained by security expenditures, including improvements to security processes?
- How do we measure the improvements?
- Are we reducing our exposure?

CSOs NEED METRICS FOR CSOs

Metrics are measures that matter, providing evidence of performance… That's why CSOs [chief security officers] are hungry for them… Security executives want to understand how their operations are working and how they can improve. CEOs want to know how the security function is faring by looking at the department's data. And metrics can provide the hard numbers and context on the performance of the security function, proving that nothing happening was the direct result of an effective security management program.

CSO
(Wailgum, 2005)

Even before major problems occur, MA can be used to watch indicators—signs of risk—that may suggest a need for different security measures. Campbell (2006b) notes that these indicators or metrics "become the earliest prompts for more in-depth analysis of trend dynamics," allowing CSOs to "look at the root causes of problems, not just the symptoms." He lists several trends that metrics may help identify:

- More frequent or more severe accidents, crimes or policy infractions;
- Increased downtime of critical equipment;
- Rise in negative background investigations;
- Changes in security response times;
- Reduction in building evacuation exercises; and
- Rise in misconduct cases within a business unit.

With careful analysis of the right metrics, a security professional can devise appropriate strategies to reduce risks. Expanding on the example of increased misconduct cases, Campbell (2006b) suggests that further investigation might show poor supervision of employees in that unit, as well as little employee awareness of company policies on business conduct. Solutions would require efforts by the security, human resources and legal departments.

MA can also be used for external comparisons—that is, comparing one organization's security-relevant metrics to those of other organizations. This process of benchmarking depends on the availability of metrics and, of course, the underlying data that must be collected to produce those metrics.

Metrics as Marketing for the Security Program

In their definition of security metrics management, Kovacich and Halibozek (2005) emphasize both the operational aspects of metrics (discussed above) and the business aspects of metrics. On the business side, they note:

> Through the use of metrics, the security cost versus benefit analysis becomes more quantitative and easier to understand and communicate in common business terms. Metrics help the security professional and others better understand the efficiency and effectiveness (value) of an assets protection program.

METRICS PROVIDE ANSWERS

Consider this: Does your management want to be able to clearly see whether you are conforming with corporate values and policies? Would they like to have a visual representation of the state of the company's risk—desirable or undesirable? Would they like to have measurements and data at hand that show whether the company is in compliance with applicable laws and regulations? Do they want to know whether past and current security investments have resulted in decreased risk or fewer incidents, so they can more easily determine the direction of future investment?

(Campbell & Blades, 2009)

That definition hints at the power of metrics and analysis (MA) to demonstrate a security department's contribution to overall corporate success. The message continues to be emphasized in prominent security forums. For example, in a presentation titled "The Security Metrics Challenge" at the 2011 ASIS International Seminar and Exhibits, speakers stressed the indispensability of metrics:

- "It's about the value proposition. If you can't show value in industry, then you are not going to go very far… Are you producing something that's going to increase or sustain the value of the company? This is very important in the boss's view."

  James Shamess, CPP, Senior Adviser for Security Policy and Oversight, Office of the Administrative Assistant to the Secretary of the Air Force

- "When you talk to senior executives, you have to talk in language they understand: money, what's the return on investment, and what's the benefit to me?… Security professionals, to have a seat at the table, need to be seen as value-added and cost-effective. You need to be able to report meaningful, intelligent, risk-based performance metrics to build confidence in your executive teams… Use those metrics to create a business case and measure program success. You have to show success in measurement. You can't just provide metrics for the sake of metrics."

  Klaus Heerwig, Director of Security, SRA International

When *Security Management* magazine gathered five leading security professionals to discuss challenges and trends in the security field, the topic of return on investment, or ROI, came up quickly. When asked how to make the business case for security, Chad Callaghan, CPP, Vice President, Enterprise Loss Prevention, Marriott International, Inc., replied (Harowitz, n.d.):

> For us, it's metrics. Having something you can measure, that you can show improvement in year over year that attaches to something that has intrinsic value to your company. Because we do safety and security both and because we are part of risk management, we're able to measure total losses to the company and that has a huge impact. It is one of the key metrics used, and it gets a lot of attention.

Brian Tuskan, Microsoft Corporation's Senior Director of Global Security Technology & Investigations, notes that by using security-

When you talk to senior executives, you have to talk in language they understand: money, what's the return on investment, and what's the benefit to me?… Security professionals, to have a seat at the table, need to be seen as value-added and cost-effective. You need to be able to report meaningful, intelligent, risk-based performance metrics to build confidence in your executive teams… Use those metrics to create a business case and measure program success. You have to show success in measurement. You can't just provide metrics for the sake of metrics.

Klaus Heerwig, Director of Security, SRA International

focused incident management software (Perspective by PPM 2000) to track and analyze laptop computer thefts, his organization has been able to identify trends, change its security approach and cut theft losses in half. Use of such software has helped Microsoft thwart or prevent major theft trends, with savings running in the high hundreds of thousands of dollars to millions of dollars (PPM 2000, 2012).

The ROI is substantial. The investment in software is modest, and the returns include:

- Loss reduction (e.g., fewer laptops stolen);
- Labor savings (more efficient data collection and report management);
- Increased efficiency;
- Intelligent resource allocation; and
- Unknown numbers of prevented high-impact incidents.

What might a detailed metrics-based ROI calculation look like? Bonnie Michelman, CPP, Director of Police, Security & Outside Services, Massachusetts General Hospital, and 2001 President of ASIS International, describes a case study of a small corporation that conducted 63 investigations one year (Michelman, 2011). Investigators recovered $1 million, and they estimate they prevented $5.5 million in future losses. Looking at recoveries alone (leaving out the value of future losses prevented), with an investigator cost of $250,000, the investigations provided an ROI of 300 percent.

CSOs can use MA to reduce a range of corporate risks. Campbell (2006a) identifies four categories of risks that businesses face: strategic, organizational, financial, and operational risks. He observes:

> It is only because there are unacceptable risks that the cost of a security program is tolerated. Risk management is the process of identifying and understanding applicable risks and taking informed actions to reduce potential failure, achieve business objectives and decrease business performance uncertainty.

The connection between security and risk management should be made clear when CSOs inform executive management about their programs. Security's valuable role in risk management can be demonstrated most effectively through metrics.

Risk management is the process of identifying and understanding applicable risks and taking informed actions to reduce potential failure, achieve business objectives and decrease business performance uncertainty.

Security's valuable role in risk management can be demonstrated most effectively through metrics.

Developing Specific Metrics

What, exactly, CSOs should measure in their metrics and analysis (MA) efforts is not obvious. Choosing metrics requires careful consideration, as the metrics must be relevant to the particular organization and its vulnerabilities. For example, in the context of business continuity planning, Heerwig (2011) observes:

> When you design metrics for your organization and present them to executive management, make sure you're doing it as it applies to your company. Don't just go out and say, 'This is the greatest threat to industry today.' Find out what affects your organization.

Typically, CSOs practicing MA collect and analyze a wide range of metrics. Doing so helps in developing an accurate picture of what is actually happening in the organization. As Heerwig states, "How do you measure 'what if'?... It's hard to report measurements when sometimes the true measurement is that nothing happened." Using numerous indicators makes it possible to compensate for the challenge of proving that security actions prevented future losses.

To create a list of metrics to collect and analyze, Treece and Freadman (2010) suggest that CSOs "list... core security missions and then determine what activities are involved in getting those things done."

Campbell (2006a) lists several hundred possible security metrics that may be relevant to a company's cost, risk, ROI, legal, policy and life safety issues. The following are just a few examples:

Security cost per square foot

Losses per square foot

Security cost per company employee

Security cost as percentage of total revenue

Increase or decrease in insurance cost due to safeguards or losses

Total losses

Number of employees involved as subjects of investigations as percentage of employee population

Number of internal investigation subjects who indicate a lack of knowledge of the policy they are accused of violating

Number of hostile workplace incidents in specific organizational units

Investigative case aging

PRODUCTS OF ANALYSIS

By analyzing collected metrics, a security professional can:

- Illustrate findings.
- Issue reports.
- Plan preventive measures.
- Create corrective action summaries.
- Make knowledge-based decisions.
- Demonstrate ROI.

Cost of downtime in critical business processes

Information security violations

Inventory shrinkage

Fines paid for false alarms

Incident response times

Percentage of personnel with known derogatory background issues hired versus not hired

Number of personnel not background-investigated before hire

Background investigation cost per case

Rate of unfavorable background investigations

Percentage of positive preemployment drug tests

Number of business relationships established without due diligence investigation

Derogatory findings from post-contract award examination

Terminations for cause as a percentage of employee population

Investigations per investigator

Recoveries per investigator

Number of nuisance alarms

Security personnel: hours of pre- and post-assignment training

Number of security vulnerabilities reported by patrol officers

Number of workplace violence incidents per X number of employees

Percentage of inactive computer user accounts that have been disabled in accordance with policy

Percentage of mobile information devices with automatic protection

Percentage of security incidents that exploited existing vulnerabilities that have known solutions

Number of security incidents that should have been but were not reported to security department

Number of safety hazards proactively identified and eliminated annually

Campbell further recommends that CSOs maintain a "dashboard" of the most important metrics, a quick-view means of gauging some of the most important security concerns in the company. These might be half a dozen "survival metrics"—metrics that are vital to the organization's success or of special concern to management. For example, a financial services company "might be particularly attuned to the number of business units with dated contingency plans and inadequate software patch administration, internal misconduct or numbers of people hired with known

Campbell further recommends that CSOs maintain a "dashboard" of the most important metrics, a quick-view means of gauging some of the most important security concerns in the company. These might be half a dozen "survival metrics"—metrics that are vital to the organization's success or of special concern to management.

derogatory backgrounds." The key to a good dashboard is to "select a few key metrics we should watch because they are the things that keep us awake at night." It may even make sense to maintain two dashboards—one for internal security use and one for monitoring issues that executive management cares about the most.

An important distinction to understand when developing specific metrics is the difference between leading, coincident and lagging indicators. A leading indicator suggests that the particular metric will be followed by a particular (but different) condition; a coincident metric suggests, for example, that if one metric is high, another condition (perhaps not directly measured) is high at the same time. A lagging indicator may confirm that a certain correlated condition existed in the past (near or far) and may still exist—the condition may not be easily measured, but the lagging indicator would prove that the condition did or does exist. In a report for the National Institute of Standards and Technology, Jansen (2009) writes:

> Analogous to economic indicators, security metrics may be potentially leading, coincident, or lagging indicators of the actual security state of the system. The distinction is significant… If a lagging indicator is treated as a leading or coincident indicator, the consequences due to misinterpretation and reaction can be serious. The longer the latency period is for a lagging indicator, the greater the likelihood for problems. That is, a lagging security metric with a short latency period or lag time is preferred over one with a long latency period, since any needed response to an observed change can take place earlier.

Examples of leading and lagging indicators in security include the following (Campbell, 2009):

- Unresolved nuisance alarms: leading indicator of future risk.
- Reduced false and nuisance alarm rates: lagging indicator of efforts to improve alarm system reliability.
- Hiring despite unfavorable background investigation: leading indicator of integrity issue.
- Reduction in number of security responders: possible leading indicator of excessive response times.

Of course, leading indicators—those "measurable factors that change before the risk starts to follow a particular pattern or trend" (Campbell, 2009)—do not justify an automatic response but must be analyzed carefully.

LEADING:

A leading indicator suggests that the particular metric will be followed by a particular (but different) condition.

COINCIDENT:

A coincident metric suggests, for example, that if one metric is high, another condition (perhaps not directly measured) is high at the same time.

LAGGING:

A lagging indicator may confirm that a certain correlated condition existed in the past (near or far) and may still exist—the condition may not be easily measured, but the lagging indicator would prove that the condition did or does exist.

Essential Ingredient: Data

The practice of metrics and analysis (MA) requires, as its basic ingredient, data concerning security-significant issues. CSOs who are already collecting data possess a valuable resource that they can mine to guide their decision making and gain support for their programs.

For CSOs who are not already collecting data, or who are doing so in ways that do not facilitate analysis, incident management software is one of the foundations for effective MA and an inherent part of the risk management cycle. Programs designed specifically for the security field can make the gathering of security-significant data orderly, convenient, and accurate—and hold the data in a format that facilitates analysis.

For example, Perspective by PPM 2000 is security-focused incident management software that incorporates activity tracking, incident reporting, investigation management and case management. By presenting users with carefully designed input forms and selection fields, the program collects essential data uniformly and completely. In addition to being designed for the security field, it can be custom-configured to a company's particular needs and terminology based on industry standards, legislation (such as Sarbanes-Oxley or the Clery Act) or corporate direction. In addition to having security personnel collect data, the corporate security department may opt to enlist other divisions (such as health and safety, human resources, audit or IT) in collecting and tracking data. Inviting non-security employees into the process—as part of an enterprise-wide MA approach or security awareness program—enables employees, either anonymously or not, from numerous sites to input incidents and other data, thereby casting a wider net in the data collection process.

For example, Brian Tuskan, Microsoft Corporation's Senior Director of Global Security Technology & Investigations, notes (PPM 2000, 2012):

> Perspective features a Web-based module (e-Reporting) so that non-security employees can file incident reports online, by themselves. We have a total workforce of over 90,000 full-time employees and thousands more that come and go through the Microsoft campuses. With such large numbers, there are inevitably losses, thefts and suspicious circumstances. With Perspective, all of these people have become part of the security reporting process.

Security-focused incident management software offers both the standardization and consolidation of data. Both of those features are vital for later analysis and reporting.

Programs designed specifically for the security field can make the gathering of security-significant data orderly, convenient, and accurate—and hold the data in a format that facilitates analysis.

Security-focused incident management software offers both the standardization and consolidation of data. Both of those features are vital for later analysis and reporting.

Such software can also automate the task of analysis, which is addressed in the next section. For example, Perspective can generate customized statistical reports, trending insights and predictive analysis.

From Data to Information: Analyzing Metrics

The second part of a metrics and analysis (MA) program is, obviously, analysis, which is the stage that leads directly to important understandings that might not otherwise be possible. Treece and Freadman (2010) specify three reasons analysis is important:

- It shows the accomplishments of the security mission.
- It leads to an understanding of why specific metrics may be different from one period to another. For example, metrics may show that security guard overtime ran high in the previous quarter, but analysis may show that a large, aggressive political rally near the site necessitated extra security.
- It provides the CSO with figures that can be used to gain support, resources or recognition for exemplary performance by security staff.

With the right analytical software, such as the business intelligence components of Perspective, a CSO can easily and constantly analyze the data on security activities, losses and investigations, viewing graphs and charts that are generated automatically. Statistics that could take days or weeks to prepare using conventional database queries are available instantly, as all the formulas and queries are built in.

For example, by using analytical software, a CSO can automatically retrieve core business statistics that answer questions like these:

- What types of incidents are occurring the most, and how much are they costing the company?
- Is the company on track to reduce incidents by 30 percent from last year?
- Are losses for a particular site up, down or steady?
- Where are incidents and losses occurring with the highest frequency and greatest impact?
- On what days and times might more security officers be required?
- Have countermeasures instituted in the previous quarter taken effect yet?

Three reasons why analysis is important:

- It shows the accomplishments of the security mission.
- It leads to an understanding of why specific metrics may be different from one period to another.
- It provides the CSO with figures that can be used to gain support, resources or recognition for exemplary performance by security staff.

The idea is to strategically analyze the metrics collected to develop business intelligence.

An especially valuable product of automated metrics analysis is trend spotting. Even with the right metrics on hand, identifying trends with the naked eye is not necessarily easy. Analytical software can bring trends to the foreground, helping a CSO identify problems accurately and then implement suitable security responses.

For example, analysis of key metrics might tell the CSO that laptop thefts have been rising at one corporate site but not others. Without analysis, a simple count of laptop thefts across the corporation might not suggest any particular countermeasure. In fact, total corporate laptop thefts could be down, even though thefts at one site were up. Once the analysis pinpoints the specific trend—that thefts are up at only one particular site—the CSO can intelligently choose the right steps to address the problem, such as investigation, employee security awareness briefings or improved locking methods.

Using the same example, analysis software can also point out correlations between the thefts and certain days of the week or times of day, employee turnover or other factors that might suggest appropriate, tailored security measures.

Analysis software points out trends and correlations that strengthen decision making within the security operation. It also produces charts and reports that are useful in demonstrating the value of the security program to others. Treece and Freadman (2010), describing metrics and analysis at the Massachusetts Port Authority, note:

> [O]ur metrics over the years... have grown to include some 229 information line items that cover everything from direct and indirect security program costs to the uptime percentages of key security equipment, like surveillance cameras... [W]e use a quarterly Security Scorecard to show what we are getting for our (currently) $68 million annual investment in security... We have found that collecting monthly and reporting quarterly allows us to have month to month data in case we need it, while only having to produce the reports four times a year.

An especially valuable product of automated metrics analysis is trend spotting. Even with the right metrics on hand, identifying trends with the naked eye is not necessarily easy. Analytical software can bring trends to the foreground, helping a CSO identify problems accurately and then implement suitable security responses.

Getting Started

The case for using metrics and analysis (MA) in security management appears strong, yet it may be hard to overcome inertia and start the process. Campbell and Blades (2009) identify two barriers to getting started: (1) no request from executive management; and (2) budget concerns.

The first potential hurdle—that management has not made a specific request that the corporate security department initiate a metrics and analysis program—should be irrelevant to a professional CSO. Executive management may not know that MA is the best way to obtain good results, but, as Campbell and Blades note,

> It does not matter why management is not asking us for metrics. We should be providing them. As the security experts, it is our job to manage risk and to inform management on our status. We should be taking metrics to them— we should not have to wait to be asked.

A second potential hurdle, the cost of undertaking the metrics and analysis approach, is also less of a challenge than it might first appear. As Campbell and Blades (2009) observe,

> If you conduct afteraction reviews, if you speak to your peers about trends and best practices, if you assess your risk on a regular basis, if you track project status or log incidents, you already have the necessary data.

Security-focused MA software can make the process efficient enough to obviate any need for a dedicated metrics-producing employee. With the right software, data can be collected and input by numerous staff members, leaving CSOs time to conduct the necessary analysis.

Once the hurdles are recognized as irrelevant or insignificant, a CSO can take steps to start the MA program. Campbell and Blades (2009) list five key steps in implementing such a program. The first step is to "identify the business drivers and objectives for the security metrics program." That means considering the organization's "goals, needs, values and policies." This step also includes identifying the metrics program's objectives, which could include reducing risk exposure or demonstrating the security department's conformity with business goals or its value or cost-effectiveness.

The first potential hurdle—that management has not made a specific request that the corporate security department initiate a metrics and analysis program—should be irrelevant to a professional CSO.

A second potential hurdle, the cost of undertaking the metrics and analysis approach, is also less of a challenge than it might first appear.

The second step is to identify the various audiences for the metrics, as well as their business goals. Doing so can help in creating specific metrics. For example,

> A metric that demonstrates a business unit's inaction to correct a known, reported vulnerability could be presented to the business unit manager (to encourage [him or her] to correct the issue) or to an internal audit committee (to pre-emptively show that Security reported the problem for correction).

The third step is to list the types of data that the metrics and analysis program will require. The objective is to line up data that will lead to actionable metrics—in other words, metrics that one can analyze to "provide direction for decisions, affirm actions taken, or provide clarity for next steps. Non-actionable metrics simply count things and have little value for influencing or finding causes of risk."

The fourth step is to develop metrics that demonstrate the security department's contribution to enterprise risk management, the company's overall strategy and objectives or, ideally, both. Risk-related metrics show how the security department reduces risks to the business. Metrics focused on overall business objectives might show how new technology has reduced security officer costs or how other security measures "remove a vulnerability that could impact brand reputation and compromise customer confidence in [the company's] products or services."

The fifth and final step is to treat the data carefully, ensuring its integrity and protecting its confidentiality. Security-focused metrics and analysis software is a significant aid in this step, organizing, protecting and ensuring consistency of collected data.

Steps to starting a metrics and analysis program:

1. Identify the business drivers and objectives.

2. Identify the various audiences for the metrics, as well as their business goals.

3. List the types of data that the metrics and analysis program will require.

4. Develop metrics that demonstrate the security department's contribution to enterprise risk management.

5. Treat the data carefully, ensuring its integrity and protecting its confidentiality.

References

Campbell, George. (2006a). Measures and Metrics in Corporate Security: Communicating Business Value. Framingham, MA: CSO Executive Council.

Campbell, George. (2006b). "How to Use Metrics." CSO Online, August 1, 2006. http://www.csoonline.com/article/220980/how-to-use-metrics

Campbell, George. (2009). "Metrics for Success: Tracking Leading and Lagging Indicators," Security Technology Executive, November 2009.

Campbell, George, & Blades, Marleah. (2009). "Building a Metrics Program that Matters." SecurityInfoWatch.com. http://www.securityinfowatch.com/Security+Executive+Council/1310623

Carnegie Mellon University. (1995). "Security Metrics," in Systems Security Engineering - Capability Maturity Model. http://www.sse-cmm.org/metric/metric.asp

Daly, Ken. (2011). "Corporate Performance Metrics to Top Board Agendas," Financial Executive, January/February.

Davenport, Thomas. (2009). "Make Better Decisions," Harvard Business Review, November.

Davenport, Tom, & Harris, Jeanne. (2010). "Analytics and the Bottom Line: How Organizations Build Success." Key Learning Summary published by Harvard Business Review.

Harowitz, Sherry. (n.d.). "Challenges and Trends." Security Management online. http://www.securitymanagement.com/article/challenges-and-trends

Hayes, Bob, & Kotwica, Kathy. (2011). "Benchmarks Aren't Magic, They're Tools," Security, September.

Heerwig, Klaus. (2011). Presentation within "The Security Metrics Challenge" at the 2011 ASIS International Seminar and Exhibits, September 20, 2011, Orlando, FL.

Hodgin, Kim. (2011, July 26). Interview with author Peter Ohlhausen.

Jansen, Wayne. (2009). Directions in Security Metrics Research. Gaithersburg, MD: National Institute of Standards and Technology, NISTIR 7564.

Kohl, Geoff. (2009). "Measuring the Business Value of Security." SecurityInfoWatch.com. http://www.securityinfowatch.com/root+level/1286197

Kovacich, Gerald, & Halibozek, Edward. (2005). Security Metrics Management: How to Manage the Costs of an Assets Protection Program. Waltham, MA: Butterworth-Heinemann.

Michelman Bonnie, CPP. (2011). "Business Case for Security: Creative Ways to Show Security's Proposition and Profitability," a presentation at the 2011 ASIS International Seminar and Exhibits, September 19, 2011, Orlando, FL.

National Institute of Standards and Technology. (2008). Information Security. NIST: Gaithersburg, MD.

Musser, Raymond. (2011). Presentation within "The Security Metrics Challenge" at the 2011 ASIS International Seminar and Exhibits, September 20, 2011, Orlando, FL.

Payne, Shirley. (2006). "A Guide to Security Metrics." SANS Institute. http://www.sans.org/reading_room/whitepapers/auditing/guide-security-metrics_55

PPM 2000. (2009). Webinar: INSTANT Business Intelligence and Statistical Reporting. http://www.ppm2000.com/downloads/Webinar-recording/Webinar-Focal-Point-Aug09.wmv

PPM 2000. (2010). Webinar: Security's ROI: How to Deliver Metrics That Reveal Trends and Justify Budgets. http://www.ppm2000.com/downloads/LiveSeminar/SecuritysROI.wmv

PPM 2000. (2012). "Optimizing Resources, Shrinking Losses—Perspective at Microsoft's Global Security Operations Centers." http://www.ppm2000.com/downloads/Case_Studies/resources/case-studies/microsoft.asp

Shamess, James. (2011). Presentation within "The Security Metrics Challenge" at the 2011 ASIS International Seminar and Exhibits, September 20, 2011, Orlando, FL.

Treece, Dennis, & Freadman, Michele. (2010). "Metrics Is Not a Four-Letter Word," Security, November.

Wailgum, Tom. (2005). "Metrics for Corporate and Physical Security Programs," CSO, February.

PPM 2000 Inc.
10088 - 102 Avenue, Suite 1307
Edmonton, Alberta T5J 2Z1

1-888-776-9776
information@ppm2000.com
www.ppm2000.com

Microsoft Partner
Gold Independent Software Vendor (ISV)

Copyright © 2012 PPM 2000 Inc. All rights reserved.
PPM 2000, the PPM 2000 logo and DispatchLog are registered trademarks of PPM 2000 Inc. Perspective by PPM 2000, the Perspective by PPM 2000 logo, Perspective e-Reporting, Perspective Focal Point, Perspective Mobile, Perspective Visual Analysis and Perspective Workflow are trademarks of PPM 2000 Inc. Microsoft and the Microsoft Gold Independent Software Vendor (ISV) Partner logo are trademarks or registered trademarks of Microsoft Corporation in the United States and other countries. All other brands, names or trademarks mentioned may be trademarks of their respective owners. Printed in Canada 03/12.